مركز البحوث والدراسات

دليل المسئول التنفيذي لحوكمة تقنية المعلومات

تحسين عمليات النظم من خلال إدارة الخدمة وكوبيت وآيتل

تأليف

روبرت ر. مولر

ترجمة

أ. محمد أحمد عبداللطيف - أ. عبدالله حسن كامل

راجع الترجمة

د. محمد بن عبدالله الشنيفي

بسم الله الرحمن الرحيم

مركز البحوث والدراسات

دليل المسئول التنفيذي لحوكمة تقنية المعلومات

تحسين عمليات النظم من خلال إدارة الخدمة وكوبيت وآيتل

تأليف
روبرت ر. مولر

ترجمة
أ. محمد أحمد عبداللطيف - أ. عبدالله حسن كامل

راجع الترجمة
د. محمد بن عبدالله الشنيفي

١٤٤٠هـ - ٢٠١٩م

بطاقة الفهرسة

ⓒ معهد الإدارة العامة، ١٤٤٠هـ.

فهرسة مكتبة الملك فهد الوطنية أثناء النشر.

دليل المسئول التنفيذي لحوكمة تقنية المعلومات تحسين عمليات النظم من خلال إدارة الخدمة وكوبيت وآيتل.

أ - روبـرت ر. مول؛ محمد عبداللطيف؛ عبدالله كامل - الرياض، ١٤٤٠هـ

٦٧٢ ص؛ ١٧سم × ٢٤سم.

ردمك: ٦-٢٨٧-١٤-٩٩٦٠

١- تقنيـة المعلومـات. ٢- تخزين واسـترجاع المعلومات ٣- الحوكمـة أ. عبداللطيف؛ محمـد (مترجم) ب. كامل، عبدالله (مترجم)

ج- العنوان.

ديوي ٠٢٥,٠٤   ١٤٤٠/٢٩٥١

رقم الإيداع: ١٤٤٠/٢٩٥١

ردمـــــك: ٦-٢٨٧-١٤-٩٩٦٠

هذه ترجمة لكتاب:

Executive's Guide to IT Governance

Improving Systems Processes with Service Management

COBIT, and ITIL

ROBERT R. MOELLER

إهداء

إهداء لأفضل صديقة وزوجة، لويس مولر.

كانت لويس رفيقتي وشريكتي لأكثر من ٤٠ عاماً، ســواء على مركبنا الشراعي في بحيرة ميشــيغان، أو في التزلج في ولاية يوتا أو في أي مكانٍ آخر، أو أثناء زيارة المتاحف أو السفر إلى أماكن ممتعة حول العالم أو في بستنة الخضروات في الفناء الخلفي للمنزل أو مشاركتي إياها في طبخ أكلات من نتاج ما زرعناه.

٦

قائمة المحتويات

مقدمة

في ظـل الظروف الاقتصاديـة الدائمة التغير التي يشـهدها عالم اليوم والأنشـطة التنظيمية المتزايـدة، تصبح الحوكمة ذات أهميـة متزايدة لجميع الشركات على اختلاف أحجامها، سـواء كانت مؤسسـات قطاع عام غير ربحيـة أو كيانات خاصة. وتتكون مفاهيم حوكمة المؤسسـات من سلسـلة من مجالات واسـعة تغطي أنشطة المؤسسـة التي تبدأ بالمسـاءلة الإدارية وإدارة المسـئوليات الائتمانية تجاه عملائها وموظفيها ومنظميها وغيرهم من أصحاب المصالح جميعهم. ويتطلـب ذلك تطبيق عدد من الإرشـادات والبرامج لضمان نزاهة الإجـراءات الإدارية وحماية المؤسسـة من الممارسـات المخالفة والاحتيالية. كما تشـتمل حوكمة المؤسسة أيضاً على عمليات الإدارة وسياسـاتها التي تعزز الكفاءة الإستراتيجية والاقتصادية للمؤسسة. وتتضمن إدارة الكفاءة الاقتصادية للمؤسسة الكيفية التي من خلالها ينوي نظام الحوكمة لديها تحسين النتائج وتحقيق الأهداف المرجوة، كما يدعو تعزيز الكفاءة الإستراتيجية للمؤسسة إلى تعزيز أهداف سياسة عامة للمؤسسة وإرسائها، تلك الأهداف التي لا تقاس دائماً من المنظور الاقتصادي مباشرةً لكنها تشتمل على أمور مثل وضع برنامج أخلاقيات مؤسسية قوي وتحسين الجودة ورفاهية الموظفين.

ومـن الطبيعي أن تحتاج الحوكمة المؤسسـية الفعالة إلى مهـارات إدارية قوية لاتخاذ قرارات مهمة وتشكيل القيادة. كما تحتاج وبشكل كبير إلى نظم وعمليات تقنية المعلومات على وجه الخصوص. ويمثل هذا المجال المهم، حوكمة تقنية المعلومات، الموضوع الشـامل لهذا الدليل التنفيذي.

وفي الأيـام الأولى لعمليـات تقنية المعلومـات ونظمها، كانـت الإدارة العليا للعمليات التشغيلية غالباً ما توكل عمليات كثيرة من عمليات تقنية المعلومات للمتخصصين المسؤولين عن بناء موارد تقنية المعلومات في المؤسسـة وتشغيلها وصيانتها. وبينما كثر الحديث وقتها عن ضرورة إشراك الإدارة ومستخدمي نظم تقنية المعلومات مع متخصصي ومطوري موارد تقنية المعلومات، فإن إدارة العمليات كانت تتعرض دائماً لخيبات أمل. فالمبادرات الجديدة لتقنيـة المعلومات وقتها لم تحقق في الغالب أهدافها المرجوة المعتمدة أو حققتها في وقت متأخـر أو احتوت على نقاط ضعـف في أمن المعلومات والرقابة الداخليـة، أو أنها لم تعد مطلوبة إما بسبب سوء التخطيط أو تقديرات احتياجات الإدارة. ولتحسين تلك الأمور اليوم، تظهـر الحاجة إلى عمليات أفضل لإدارة وتنسـيق جميع جوانب موارد تقنية المعلومات في المؤسسة، أي الحاجة إلى حوكمة تقنية المعلومات.

هــذا الكتاب هو دليل للســلطة التنفيذية يتنــاول هذا المفهوم المهــم لحوكمة تقنية المعلومــات. ولا نركز هنا عــلى قيام متخصصي تقنية المعلومــات بتركيب معدات هاردوير وبرمجيات وتوصيلات شبكات خاصة بتقنية المعلومات، ولا على الموارد المهمة مثل المدققين الداخليــين الذين يختبرون عمليات تقنية المعلومات ويراجعونها. لكننا نركز على الســلطة التنفيذية في المؤسسة التي يكون لديها بعض الفهم لعمليات تقنية المعلومات، لكنها تكون مهتمــة أكثر بمعرفة المزيد عن القضايــا والعمليات الضرورية المهمة في إدارة موارد وأنظمة تقنية المعلومات بكفاءة وكذلك الاستفادة منها في بيئة اليوم المتصلة بالإنترنت.

ويهدف هذا الكتاب إلى تقديم معلومات أساســية عالية المســتوى عن نوع من القضايا المتعلقــة بحوكمة تقنية المعلومات التي تعتبر مهمة لمؤسســات الأعمال وللمدير التنفيذي اليوم. ونأمل أن نزود الجهة التنفيذية في المؤسسة بمعلومات عامة وكافية تتمكن من خلالها مــن تكوين فهم أكبر عن قضايا حوكمة تقنيــة المعلومات المهمة هذه الأيام ولتكون قادرة أيضاً على طرح أســئلة أفضــل لتحقيق فهم أكبر لهذه القضايا ولاتخــاذ قرارات فعالة فيما يتعلق بمســائل حوكمة تقنية المعلومات تلك. فعلى ســبيل المثال: نشير اليوم في كثير من الأحيان في أدبيات الأعمال التجارية إلى مصطلح الحوسبة السحابية (Cloud Computing). وســيقدم لنا الفصل التاسع نظرةً عامةً عن الحوسبة الســحابية وسبب أهميتها في حوكمة تقنية المعلومات الفعالة. وبالمثل، سنقدم مفهوم اتفاقيات مستوى الخدمة (SLAs)، وهي عادةً عقود غير رسمية تُبْرَم بين مستخدمي أو أصحاب موارد تقنية المعلومات وإدارة تقنية المعلومات. وهدفنا هنا هو مســاعدة السلطة التنفيذية في المؤسسة ليكون لديها فهمٌ أكبر عن سبب أهمية اتفاقيات مستوى الخدمة وكيفية تبنيها في المؤسسات وإدارتها على اختلاف أحجامها وأنواعها، وكيف يمكن استخدامها لتحسين عمليات حوكمة تقنية المعلومات.

وقد قُســمت فصول هذا الكتاب لســتة مواضيع أو أجزاء رئيســية. كل جزء من هذه الأجــزاء والفصول التي يحتويهــا يعتبر وحدة متكاملة في العمــوم، ويلخص قضايا حوكمة تقنيــة المعلومات التــي تخص هذا الجزء، ونأمــل أن تتمكن من خدمــة الجهة التنفيذية بالمؤسســة من خلال تزويدها بمعلومات كافية عالية المســتوى لفهم كل من قضايا حوكمة تقنية المعلومات تلك ومفاهيمها.

الجزء الأول: مفاهيم حوكمة تقنية المعلومات:

تزودنا فصول هذا الجزء بمقدمة شاملة عن مفهوم حوكمة تقنية المعلومات وكيفية تطبيقها على مؤسسات الأعمال عموماً، وعلى موارد تقنية المعلومات لهذه المؤسسات لاحقاً. ويحتوي هذا الجزء على فصل يصف أهمية قواعد قانون ساربينز أوكسلي (Sarbanes-Oxley Act (SOx) rules) وتأثيرها بوصفها مجموعة من التشريعات تحوي القواعد العامة لضبط المؤسسات المالية وغيرها من نظم الرقابة الداخلية التى وضعت للمرة الأولى في الولايات المتحدة بدايات هذا القرن، أما الآن فهي مستخدمة تقريباً في جميع أنحاء العالم. ويختتم هذا الجزء بفصل يشرح قضايا شاملة لنظام الحوكمة والمخاطر والامتثال وهي ما تعرف بقضايا جي آر سي (GRC)، وهو مفهومٌ مهمٌ ومصطلحٌ شائعٌ في العديد من النقاشات الإدارية في مؤسسات اليوم.

الجزء الثاني: أطر عمل لدعم حوكمة فعالة لتقنية المعلومات:

بالإضافة إلى المعايير والمفاهيم القيمة لحوكمة تقنية المعلومات، تحتاج الجهة التنفيذية في المؤسسة لفهم بعض أطر العمل المهمة لحوكمة تقنية المعلومات وحوكمة المؤسسة بكاملها. كما يحتوي هذا الجزء على فصل يقدم لمحة أو نظرة عامة عن إطار الرقابة الداخلية للجنة المنظمات الراعية (COSO) ويوضح سبب أهمية هذا الإطار بالنسبة لحوكمة فعالة لتقنية المعلومات. ويحتوي هذا الجزء أيضاً على فصل يقدم لمحة أو نظرة عامة ومقدمة عن أهداف ضوابط المعلومات والتقنيات ذات الصلة وهو ما يعرف بمصطلح كوبت (COBIT)، كما يدعم هذا الفصل توجيهات صادرة من معهد حوكمة تقنية المعلومات. ويمثل كلٌ من ذلك مفاهيم مهمة في الرقابة الداخلية، ويجب أن يكون المسئول التنفيذي في المؤسسة مدركاً لتلك المفاهيم ولسبب أهميتها في حوكمة تقنية المعلومات.

ويحتوي هذا الجزء أيضاً على فصل يقدم مفهوماً مهماً آخر في حوكمة تقنية المعلومات، يعرف بمكتبة البنية التحتية لتقنية المعلومات آيتل (ITIL)، وهو عبارة عن المواد الإرشادية لأفضل ممارسات إدارة جميع جوانب موارد تقنية المعلومات في المؤسسة. وسيتناول هذا الفصل أيضاً منتدى إدارة خدمة تقنية المعلومات بوصفه مرتبطاً بمكتبة البنية التحتية لتقنية المعلومات، هذا المنتدى الذي يعد منظمة احترافية هامة تقدم دليلاً إرشادياً لحوكمة تقنية

المعلومات. ويجب على المسئول التنفيذي بالمؤسسة الذي يضطلع بمسئوليات إدارة عمليات تقنية المعلومات أن يتمتع بمستوى فهم جيد لتلك المواد الإرشادية واستخداماتها في إحدى إدارات تقنية المعلومات وكيفية دعمها لحوكمة تقنية المعلومات لتكون أكثر كفاءة.

كما تقدم فصول الجزء الأول من هذا الكتاب إطارين مهمين في حوكمة تقنية المعلومات. أولاً: سنناقش عدة معايير أيزو (ISO)، المنظمة العالمية للمعايير، ومجموعة من المواد الإرشادية المهمة لحوكمة تقنية المعلومات. وسنقدم أيضاً ما يعرف بـ (OCEG) أو المجموعة المفتوحة للامتثال والأخلاقيات ومجموعة من إرشادات إدارة المخاطر. ولابد هنا من فهم كل من معايير الأيزو لحوكمة تقنية المعلومات والمجموعة المفتوحة للامتثال والأخلاقيات (OCEG) لتنفيذ ممارسات حوكمة فعالة لتقنية المعلومات. ومن المفترض أن تساعد هذه الأطر مدير الشركة على فهم بعض قضايا حوكمة تقنية المعلومات الهامة.

الجزء الثالث: أدوات وتقنيات إدارة البنية التحتية لحوكمة تقنية المعلومات:

تشمل البنية التحتية لتقنية المعلومات جميع الأشخاص والموارد اللازمة لتشغيل تقنية المعلومات في المؤسسة وإدارتها، متضمناً ذلك أجهزة الخوادم وأخصائي أمن تقنية المعلومات وجميع الأشخاص والمعدات اللازمة لإدارة شبكة الاتصالات. ويناقش فصل في هذا الجزء العديد من التقنيات الأحدث والمهمة التي تتحكم في تغير عالم تقنية المعلومات اليوم، مثل مفاهيم الحوسبة السحابية ومفهوم الافتراضية. وسنتحدث عن هذه المفاهيم وقضايا أخرى ذات صلة، كما سنناقش سبب أهميتها لحوكمة تقنية المعلومات.

وتتعرض البنى التحتية لتقنية المعلومات لنوعية من التهديدات على مستوى الأمن والسلامة، مثل تعرضها لهجوم غير متوقع من إحدى البرامج التخريبية أو عدم القدرة على استعادة الأعمال بسبب قصور في أنظمة النسخ الاحتياطي أو انتهاكات كلمات المرور مما يسبب اختراق البيانات السرية. ويوجد فصل هنا يتحدث عن قضايا مهمة لكفاءة حوكمة تقنية المعلومات، وهي قضايا تخطيط أمن تقنية المعلومات واستمراريتها. كما يوجد فصل آخر هنا يتناول بعض القواعد والأنظمة الأمنية لتقنية المعلومات الأكثر أهمية لتأسيس حوكمة تقنية معلومات ذات كفاءة عالية في المؤسسة.

ثم ننهي هذا الجزء بفصل يتناول أساليب تحقيق قيمة أكبر لعمليات تقنية المعلومات التـي يجب أن تتضمن عمليات تُدار وتُراقب بشـكل جيد وعمليات تقنية معلومات ذات كفاءة وجدوى اقتصادية. ويجب على الإدارة بجميع مستوياتها أن تتمتع بمستوى فهم عام لآلية تطبيق هذه القضايا والاسـتفادة منها. وسـيطرح هذا الفصل أيضاً بعض التوجيهات من وجهة نظر إدارة تقنية المعلومات.

الجزء الرابع: بناء أنظمة حوكمة تقنية معلومات فعالة ومراقبتها:

بالإضافة إلى أدوات وعمليات البنية الأساسـية لتقنية المعلومـات التي ذُكرت في الجزء السـابق، فإن فصول هذا الجزء تناقش طرق بناء عمليات حوكمة تقنية معلومات فعالة في النظم والتطبيقات التي تتبناها المؤسسـات. ويتناول أحد الفصول هنا بشكل خاص أهمية مـا تعرف عموماً بأنها البنيـة الموجهة نحو الخدمة (SOA)، وهي الطريقة الأكثر شـيوعاً واسـتخداماً اليـوم لبناء تطبيقات جديـدة وتنفيذها، تلك التطبيقـات التي تمثل عمليات مختلفة تماماً عن العمليات التقليدية القديمة المتبعة مسبقاً في تطوير التطبيقات. وتتناول الفصول الأخرى في هذا الجزء قضايا حوكمة تقنية المعلومات اللازمة لإدارة الأنظمة وتغيرات العمليات وضوابط المراجعة بالإضافة إلى الحديث عن الطرق المسـتخدمة في تطبيق النظم المتكاملة التي تقدم حوكمةً لعمليات تقنية المعلومات وإدارةً لها بشكل أفضل.

ويوجد فصل في هذا الجزء يتحدث عن الأدوات والوسائل المستخدمة في إدارة المشاريع والبرامج. ويجب أن تدرك الإدارة بمختلف مسـتوياتها أهمية وقيمة كل من الإدارة الجيدة للمشـاريع ووسـائل الرقابة المسـتخدمة لتعزيز عمليات حوكمة تقنية المعلومات. ويأتي الفصـل الأخير في هذا الجزء ليتحدث عن اتفاقيات مسـتوى الخدمة، حيث يتناول معايير ومقاييس الأداء الرسـمية بين موارد تقنية المعلومات ومسـتخدميها، وهي إحدى الأدوات المهمة للغاية لحوكمة تقنية المعلومات.

الجزء الخامس: متابعة وقياس حوكمة إدارة المؤسسة ومجلس الإدارة:

ركزت معظم الفصول السـابقة على تمكين المسئول التنفيذي لتقنية المعلومات من فهم وتنفيـذ عمليات حوكمة تقنية المعلومات الفعالة في عمليات تقنية المعلومات بالمؤسسـة

وأنظمتها. أما فصول هذا الجزء فتركز على دور التدقيق الداخلي في المؤسسة، حيث يحتوي هذا الجزء على فصل يوضح أهمية التدقيق الداخلي لحوكمة تقنية المعلومات.

كـما يحتوي هذا الجزء أيضاً على فصل يتناول طرق إدارة الوثائق من منظور المسـئول التنفيذي لتقنية المعلومات متضمناً أهمية قضايا حفظ محتوى البيانات وإدارتها.

الجزء السادس: حوكمة تقنية المعلومات وأهداف المؤسسة:

يركـز هذا الجزء الأخير من كتابنا على بعض الإرشـادات لوضع ثقافـة أخلاقية في بيئة العمـل ومواصلة العمل بمقتضاها، الأمر الـذي يمكن اعتباره من العناصر الهامة في حوكمة تقنية المعلومات. كما يحتوي هذا الجزء على فصل يتحدث عن أهمية تطبيقات حوسـبة شـبكة التواصل الاجتماعي – كثيرة الاسـتخدام هذه الأيام كفيسـبوك مثلاً - ومدى تأثيرها في حوكمـة تقنية المعلومـات. أما الفصل الأخير من هذا الكتـاب فيحتوي على توجيهات حول كيفية اسـتخدام حوكمة تقنية المعلومات لتحقيق القيمة المرجوة من استخدام تقنية المعلومات.

ركزت هذه الفصول على حاجات الإدارة التنفيذية العليا للمؤسسة واهتماماتها. وسنبدأ كل فصـل من الفصول التالية بالحديث عن أهمية عنوان الفصل من منظور حوكمة تقنية المعلومات. ثم سـنتحدث عن أدوات ووسـائل تنفيذ عمليات حوكمة معينة وطرق قياس مدى نجاحها. وبالإضافة إلى هذه الفصول المخصصة للحديث عن الموضوعات المحددة التي أشرنا إليها، فإن هناك فصولاً أخرى ستتناول بالشرح عناصر مهمة من عمليات إدارة خدمة تقنية المعلومات وكوبت (COBIT) وآيتل (ITIL). كما سنحاول الربط بين جميع القضايا الخاصة بحوكمة تقنية المعلومات وبين الضوابط والمخاوف العامة لحوكمة المؤسسة.

إن الهـدف العام من هذا الكتاب ليتمثل في مسـاعدة كبار مديري المؤسسـات على فهم أهمية قضايا حوكمة تقنية المعلومات بشـكل أفضل وعلى تطبيقها في مؤسسـاتهم، لتكون نتيجة ذلك الوصول إلى نظم وعمليات أقوى لكل من تقنية المعلومات والمؤسسة بكاملها.

الجزء الأول

مفاهيم حوكمة تقنية المعلومات

الفصل الأول

أهمية حوكمة تقنية المعلومات لجميع المؤسسات

كان الظهـور الأول لتطبيقات تقنية المعلومات والحاسـبات بشـكل أسـاسي في عالم الأعمال مطلع سـتينيات القرن العشرين في الولايات المتحدة وأوروبا. فقد كانت وقتها تقنية أعمال جديدة صاحبها قيام العديد من الشركات بتقديم عروض تنافسية لمنتجاتها من المعدات الحاسوبية والبرمجيات للشركات الرئيسية الكبرى ذلك الوقت. وقد سارعت الـشركات على اختلاف مسـتوياتها لمواكبة تلك التقنية الحديثة، فضلاً عن الاسـتثمارات الضخمة التي خُصصت لتثبيت نظم جديدة وتوظيف مبرمجين ومحللين لبنائها وإطلاقها وتدريبهـم على ذلـك. وعلى الرغـم من وقوع بعـض الإخفاقات على طـول الطريق، فإننا جميعاً، وفي هذه الأيام نسـتخدم تلك النوعيات مـن المنتجات البرمجية والمعدات الحاسوبية ونستفيد منها.

واليـوم نجد أن نظم تقنية المعلومات المدعمة بتقنيات دائمة التغير والتطور تعد بمثابة العنـصر الأسـاسي في الغالب لجميع أنشـطة الأعـمال. ومع ذلك، نجد أن أنشـطة تقنية المعلومات التي نمارسـها ليسـت مدعمة ببعضٍ من المعايير والإجراءات نفسـها الموجودة في مجالات أعمال أخرى. فعلى سـبيل المثال، يتم دعم نظم المحاسـبة والمعايير المالية من خلال مبادئ محاسـبية متعارف عليها يقوم بمراجعتها مدققون مسـتقلون، فضلاً عن أنها تخضع لقواعد محاسـبة مالية حكومية كقواعد هيئـة الأوراق المالية والبورصة في الولايات المتحدة الأمريكية. كما توجد قواعد مشـابهة لأفضل الممارسات والمعايير الخاصة بمجالات أنشـطة أعمال أخرى كما هو الحال في كثير من مجالات التسـويق ومراقبة الجودة. وليس هـذا هو حال عمليـات تقنية المعلومات ونظمهـا. وعلى الرغم مـن حقيقة أن عمليات تقنية المعلومات تواجه هذه الآونة متطلبات متزايدة فيما يخص الامتثال المهني والحكومي فضلاً عن تعرضها لكم هائل من مخاطر النظم المرتبطة بذلك، فإن الحاجة مسـتمرة لتبني ممارسات أفضل في حوكمة تقنية المعلومات هذه الأيام.

كان مفهــوم حوكمة تقنية المعلومات مجهولاً إلى حد كبير لعدة ســنوات قليلة مضت. فقد كنا نرى حوكمة المؤسســات من منظور الأدوار والأنشــطة التي تقوم بها الإدارة العليا ومجلــس الإدارة، في حين كنــا لا نرى إدارات تقنية المعلومات في هذه المؤسســات القديمة إلا في شــكل إدارات دعم فني مهمة للغاية وليســت أنشــطة رئيســية للأعمال. لقد تغير حقــاً مفهومنا العام حول حوكمة المؤسســات في الولايات المتحدة في الســنوات الأولى من القــرن الحالي، وذلك بعد الإخفاق الــذي تعرضت له إحدى كبرى الشركات الأمريكية والتي تدعى إنرون (Enron). الأمر الذي فاجأ الجميع ولم يكن متوقعاً على الإطلاق لدرجة قيام الهيئــات التنظيمية الحكومية في الولايات المتحدة بإجراء تحقيق في هذا الأمر واكتشــفت غياب العديد من الممارسات المالية وممارسات حوكمة الشركات. الأمر الذي أدى إلى فرض قانون ســاربينز أوكسلي [Sarbanes-Oxley (SOx)] في الولايات المتحدة الأمريكية. وقد كان لهذه القواعد التشريعية الأثر الرئيسي على الممارســات المتعلقة بإعداد التقارير المالية وحوكمة الشركات، وذلك في الولايات المتحدة الأمريكية أولاً وبعدها في جميع أرجاء العالم. وقد كان لقانون ســاربينز أوكســلي أيضــاً دور رئيسي فيما يتعلق بالحاجــة لحوكمة تقنية المعلومات بشكلٍ فعَّال.

وفي هــذه الآونة يفكر كبار المديرين ومديرو تقنية المعلومات والممارســون في حوكمة تقنية المعلومات بطــرق عديدة غير أنها مختلفة، إذ يرى البعض حوكمة تقنية المعلومات على أنها قواعد "قيادة وسيطرة" على مبادرات تقنية المعلومات، وأن واضعي تلك القواعد هــم مدققون داخليون ومديــرون تنفيذيون غير تقنيين ومستشــارون خارجيون؛ في حين يراها آخرون مجرد آلية تســتخدمها المؤسســة لتطبيق نهج الأخ الأكبر بفرض قيود تنازلية Top-Down Constraints على جميع أنشــطة تقنية المعلومات. أما من منظور ممارس تقنيــة المعلومات الذي يبني النظم ويديرها بهدف تحســين إنتاجيــة الأعمال، فإننا نجد أحيانــاً أن حوكمة تقنية المعلومات تبــدو وكأنها شرٌ لا ضرورة له يعيق النواحي الإبداعية والإنتاجيــة المرتبطة بتقنية المعلومات في المؤسســات. على كل حــال، فإن حوكمة تقنية المعلومــات لا تتحكــم في إدارة الشركة وإداراتهــا التقنية من خلال فــرض لوائح ومعايير وسياســات صارمة، لكن الحوكمة الجيدة لتقنية المعلومات في المقابل لا تعدو إلا أن تكون مجموعة من السياســات وأفضل الممارســات التي يلزم أن تعمل باعتبارها قوة إستراتيجية

تجعل من الممكن تحسين العمليات التشغيلية للأعمال، وبتلك الصورة لحوكمة تقنية المعلومات نجد جميع المؤسسات بكل مستوياتها تتبناها، بل نراها تتجاوز حدود عمليات تقنية المعلومات المؤسسية.

وتتميز الحوكمة الجيدة لتقنية المعلومات بالتوافق مع المؤسسة بشكل إستراتيجي لدعم تطوير بنية تقنية معلومات تقدم قيمة مؤسسية مناسبة يمكن تعظيمها. تساعد حوكمة تقنية المعلومات في قياس نمو الأعمال ونجاحها وكذلك قياس صحتها المالية. تقدم الفصول التالية من هذا الكتاب نظرة جديدة وشاملة لحوكمة تقنية المعلومات والتي تتناول معايير أداء الأعمال المؤسسية الجوهرية إلى جانب العوامل المهمة للالتزام بالامتثال وإدارة المخاطر. ونظراً لأن الفصول التالية ستناقش جوانب مهمة لكل من تلك العوامل، فإننا سنشير إلى الحوكمة والمخاطر والامتثال بهذا الاختصار (GRC) وهي مجموع الحرف الأول لكل كلمة. وهو المصطلح الشائع استخدامه هذه الأيام في المطبوعات المتعلقة بالأعمال.

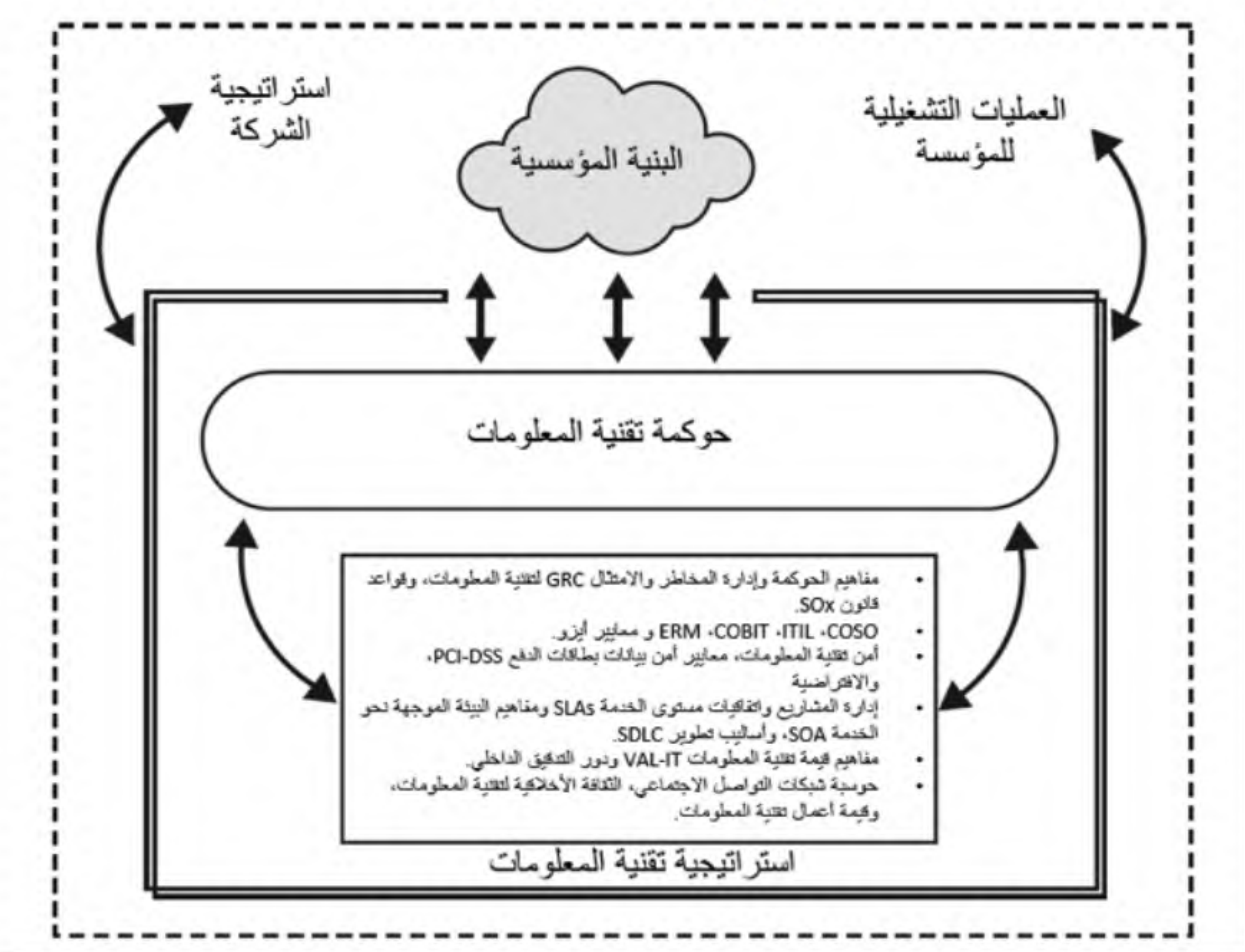
تبين حوكمة تقنية المعلومات الطريق الذي من خلاله تتمكن المؤسسة من تقديم قدرات أعمال لإنجاز مهام حرجة، وذلك باستخدام إستراتيجيات تقنية المعلومات وأهدافها وغاياتها. كما تهتم حوكمة تقنية المعلومات بتحقيق التوافق الإستراتيجي بين أهداف الأعمال وغاياتها من جهة واستغلال موارد تقنية المعلومات لديها من جهة أخرى لتحقيق النتائج المرجوة بكفاءة. يبين الشكل التوضيحي (١-١) هذا المفهوم لحوكمة تقنية المعلومات وكيفية توافقه مع جميع إستراتيجيات المؤسسة.

على الرغم من أن الشكل التوضيحي (١-١) عام جداً، إلا أنه يعرض مفاهيم حوكمة تقنية المعلومات – موضوع هذا الكتاب -في الوسط لتكون ضمن الإستراتيجيات والعمليات الشاملة للمؤسسة، وهو مفهوم أساسي دائماً يجب أخذه في الحسبان. وفي كثير من الأحيان قد يرى مدير تقنية معلومات متسلط أن أفكاره لتحسين نظم تقنية المعلومات وعملياتها وإدارتها تتجاوز في أهميتها غالباً الأنشطة الأخرى للمؤسسة، ولذا يجب علينا دائماً أن نعي أنه على الرغم من الأهمية القصوى لعمليات تشغيل تقنية المعلومات بالنسبة لجميع أعمال المؤسسة في كثير من الأحيان، فإنه يجب أن تنسجم تلك العمليات مع جميع أنشطة المؤسسة وإستراتيجياتها. وعلى الرغم من أن مدير إدارة تقنية المعلومات أو الرئيس

التنفيذي للمعلومات Chief Information Officer (CIO) ، قد يشــعر بأن لديه المقترح الأصلح لعمل بعض التغييرات أو التحســينات في عمليات تقنية المعلومات؛ فإن هذا المقترح يجب أن يكون نافعاً لباقي أنشطة المؤسسة. فعلى سبيل المثال، قد يدرك الرئيس التنفيذي للمعلومات أهمية إبرام اتفاقيات مستوى الخدمة Service Level Agreements (SLAs)، أو عقود غير رســمية ما بين مســتخدمي تقنية المعلومات ومقدميها، وهو ما ســنتناوله في الفصل الســابع عشر من هذا الكتاب، باعتبار ذلك وســيلة مناســبة لتحسين عمليات تقنية المعلومات وتطويرها. ولكن في حال عدم استحسان هذا المقترح من قِبل الإدارة العليا، فإنه يجــب على الرئيس التنفيذي للمعلومات أن يذعن لتوجه الإدارة العليا ولا يتوقف عن عمل تحسينات أخرى كلما أمكن ذلك.

شكل توضيحي (١-١)

مفاهيم حوكمة تقنية المعلومات



ولعل المقصد هنا يتركز في أن البنية المؤسسـية لتقنية المعلومات هي التي تضع جميع قواعد الإطار العام لجميع أنشـطة المؤسسـة وحوكمة تقنية المعلومات. تقدم لنا الفصول التاليـة مـن هذا الكتاب عـدة مجالات يمكن من خلالها تحسـين نظم تقنيـة المعلومات وعملياتها. لكن مع اسـتهداف تحسين حوكمة تقنية المعلومات في المؤسسة بالكامل يجب أن تنسجم تحسينات حوكمة تقنية المعلومات تلك مع الإطار العام لعمليات المؤسسة.

يشـير الجزء الخاص بحوكمة تقنية المعلومات في الشـكل التوضيحي (١-١) إلى سلسلة من الأنشطة الأخرى، يتوافق كل نشاط منها تقريباً مع موضوعات أحد الفصول الموجزة في مقدمة الكتاب والمفصلة في الفصول اللاحقة. وقد حاولنا في هذه الفصول أن نوجز العديد من القضايا المهمة لتحسـين حوكمـة تقنية المعلومات، تلك القضايـا التي يجب أن ترتبط بشكل وثيق بجميع عمليات المؤسسة.

تعمـل حوكمـة تقنية المعلومـات على توزيع السـلطة على مختلف طبقـات الهياكل التنظيمية داخل المؤسسـة مع ضمان اسـتخدام تلك السـلطة بشكل سـليم وحكيم. ولا نقصد هنا مجرد الهياكل الهرمية؛ بل يجب علينا دوماً أن نتذكر أن الهياكل الشبكية تسمح بالتخصصية وتشـكيل الفرق وتشـكيل بنية تحتية لدعم تلك الفرق. فالتخصصية تسـمح لمجمـوع أجـزاء المنظمة بأن يكون أكـبر من الكل. كما يجب أن نتذكـر أن حوكمة تقنية المعلومات ليست حكراً على المنظمات الكبرى، فالمؤسسات الأصغر تفتقر أيضاً إلى ممارسات جيدة لحوكمة تقنية المعلومات. ومع ذلك، يوجد بوضوح عدد أقل من نقاط الرقابة التي يلـزم توظيفها في عمليات المؤسسـات الصغـرى في حين أن تركيزنا في فصـول هذا الكتاب سينصب على المؤسسات الكبرى.

عندما نسـتعرض مفهوم حوكمة تقنية المعلومات كما أوردته الفصول التالية من هذا الكتاب، نجد أنها تؤثر في أداء الأعمال وتسـاعد وبشكل مثالي المؤسسة في أن تتفوق على منافسيها. ومن الموضوعات الأساسية هنا أن تعرف أن حوكمة تقنية المعلومات هي التي تحدد أداء الأعمال وخاصـة أداء موارد تقنية المعلومات وقت تطبيقها لتحقيق الأهداف الإسـتراتيجية للأعمال. فالحوكمة الجيدة لتقنية المعلومات تؤدي مباشرة إلى إنتاجية أكبر وجودة أعلى ونتائج مالية أفضل، في حين أن الحوكمة السيئة لتقنية المعلومات تؤدي غالباً

إلى إهدار برمجي وبيروقراطية وانخفاض في الروح المعنوية وتدني الأداء المالي بشكل عام.

ولإثبات أهمية الممارسـات الجيدة لحوكمة تقنية المعلومات علينا أن ننظر إلى المؤسسات التجاريـة التقليديـة التي تنتج السـلع والخدمات لعملائها التقليديـين، حيث نجد أن هؤلاء العمـلاء عموماً يـرون الأعمال فقط عندمـا يتواصلون مع تلك المؤسسـات لتقديم طلباتهم للحصـول على تلك المنتجات أو على قيمة من خلال بيـع تلك المنتجات أو إنتاجها أو لتقديم معلومات من خلال ملء الاسـتبيانات والتحليلات التسويقية. تعد كفاءة العمليات الداخلية للأعمال وتنسـيقها هي ما تشـكل خبرة العملاء بمجملها، وهذا في حد ذاته مجال من مجالات أداء الأعـمال يجب قياسـه وتطويره. وحتى تؤثر حوكمة تقنية المعلومات بشـكل إيجابي في أداء الأعمال لابد أن تركز على مجمل عمليات الأعمال تلك وتستكشـفها، تلك العمليات التي يتفاعـل معها العملاء. وفي المقابل نرى أن الحوكمة السـيئة لتقنية المعلومات تُخرِج العميل من نظرها التزاماً منها بتطبيق بعض اللوائح والقوانين والمعايير والسياسات المفضلة والمعزولة. كما نلحظ في سـياق عمليات الأعمال الشـمولية (من النهاية إلى النهاية) أن المكاسب المحلية الناتجة من كفاءة العمليات وإنتاجيتها لا تحقق في الغالب النتائج المرجوة. هذا بالإضافة إلى أن تطبيق اللوائح الخارجية على عمليات الأعمال الداخلية يجب توضيحه بطرق تؤثر إيجاباً في تجارب العملاء، ولا يكون مجرد امتثال ظاهري للوائح، إذ إن عمل ما هو خلاف ذلك سيعرض المؤسسـة للمخاطـر. فالحوكمة الجيدة لتقنية المعلومات هي التـي تتناول عمليات الأعمال الشمولية بمجملها وتقوم بتنسيق أنشطة المؤسسة مع مرور الوقت وعبر حدود المنظمة.

وكما سـنرى في فصـول هذا الكتاب، فـإن حوكمة تقنية المعلومات لا يجـب أن تُؤخذ في الاعتبـار فقط عند إطلاق المؤسسـة لمبادرة جديدة، ذلك أنها ليسـت مشروعـاً يبدأ وينتهي بشـكل منفصل، لكن يجب اعتبارها عنصراً أساسـياً في نسيج المؤسسـة يتجاوز حدود الزمن والقيادة وغيرها من المبادرات. فسواء كانت عمليات حوكمة تقنية المعلومات في المؤسسة قد تطورت بشـكل غير مقصود نتيجة للعمليات التحسينية والتطويرية أو بشكل مقصود نتيجة لمشروع مدروس، فإن الأسـئلة التي يجب أن يسـألها المدير الأول (الأعلى) هي: إلى أي مدى كانت عمليـات حوكمة تقنية المعلومات التي أجريها مفيـدةً في عملية تقديم قيمة للأعمال الإستراتيجية بشكل فعال عاماً بعد عام؟ وهل العمليات التي أجريها يمكن تكرارها والتنبؤ بها وتعظيمها؟ وهل هي تلبي حقاً احتياجات أعمالي وعملائي (بعيداً عن تبني تقنية المعلومات)؟

ومن غير المرجح أن تصلح عملية حوكمة تقنية معلومات واحدة لخدمة جميع أعمال تقنيــة المعلومات في المؤسســة مقارنــة بصلاحيتها لخدمة كل عميل من عملاء المؤسســة بحيث يكون راضياً تماماً عن المنتج نفسه أو عن تهيئة تقديم المنتج أو الخدمة التي تنتجها المؤسســة. ونتيجة لذلك، يلزم أن نأخذ في الاعتبار عــدداً من العمليات المرتبطة بحوكمة تقنيــة المعلومــات. إن هذه المجموعــة المتكاملة من عمليات حوكمــة تقنية المعلومات المتاحــة هي ما نطلق عليه في فصول هذا الكتاب اســم الصــورة الكاملة الكبيرة لحوكمة تقنية المعلومات (IT (Governance Landscape.

إن حوكمة تقنية المعلومات ما هي إلا مجموعة جزئية من حوكمة المؤسسة، حيث تقوم وعلى أعلى مســتوى بتحديــد الاحتياجات التي يجب إنجازها من خلال تحســين العمليات الإدارية الشــاملة. وتحيــط حوكمة تقنية المعلومات ذاتياً بالنظم والبنية التحتية الشــاملة لتقنيــة المعلومات والاتصالات. إن حوكمة تطوير منتج مــا، مثل حوكمة تقنية المعلومات، تعتــبر مجموعــة فرعية من حوكمة المؤسســة وتتداخل مع حوكمة تقنيــة المعلومات. ولا تستهدف استخدام حوكمة تطوير المنتجات إلا المؤسسات التي تطور المنتجات (خلافاً لتقديم خدمــة تقنية المعلومات الوارد تناولها في الفصل الســابع عشر من هذا الكتاب على ســبيل المثــال). ولذلك ينبغي تطبيق حوكمة تطوير تقنيــة المعلومات في إدارات وبرامج التطوير، تلك الحوكمة التي تعتبر مجموعة فرعية من حوكمة تطوير تقنية المعلومات والمنتجات.

تقــدم الفصــول التالية من هــذا الكتاب وتصف لنــا عدة أطــر ومفاهيم مهمة، بمســميات مثل كوبت (COBIT) وآيتل (ITIL)، يفهمها جيداً المتخصصون في تقنية المعلومات أكثر من المديرين التنفيذيين في المؤسســة. وعلى كل حال، فكل تلك الأمور تعتــبر بمثابة أدوات وعمليات مهمة لتحســين حوكمة تقنية المعلومات في المؤسســة وتطويرها، كما سيناقش الفصل الثاني. وفي عالمنا المتمركز حول تقنية المعلومات اليوم يجب أن تدرك الســلطة التنفيذية العليا في المؤسســة أهمية حوكمة تقنية المعلومات ومفاهيم أنشــطة الامتثال وإدارة المخاطر المرتبطــة بتقنية المعلومات. وهو ما يعتبر الهدف العام لهذا الكتاب.

الفصل الثاني

المفاهيم الأساسية للحوكمة وقواعد قانون ساربينز أوكسلي SOx

كما ناقشنا في الفصل الأول فإن مصطلح حوكمة تقنية المعلومات المؤسسية ليس بالمصطلح الجديد، لكنه عبارة عن مفهوم له معاني مختلفة بالنسبة لأشخاص مختلفين. وقد استمر تطور مفهوم الحوكمة المؤسسية خلال السنوات الأخيرة خاصة في الولايات المتحدة. واستجابة لسلسلة من عمليات الاحتيال والإخفاقات التي كانت قد تعرضت لها المؤسسات خاصة في العقود الأخيرة من القرن الماضي، فقد كان هناك تركيز كبير على عملية تحسين مدونات قواعد السلوك في المؤسسة وإنشاء ما يسمى بإدارات أخلاقيات العمل. وقد شارك مؤلف هذا الكتاب في قضايا حوكمة الشركات عندما أُوكل إليه إدارة التدقيق الداخلي في واحدة من كبرى الشركات الأمريكية، حيث طُلِبَ منه أن يرأس فريق العمل ويقود الشركة للقيام بمراجعة العديد من القواعد الداخلية وإعادة صياغة مدونة القواعد السلوكية واستحداث إدارة لمتابعة أخلاقيات العمل في الشركة. وقد كان ذلك استجابة للتهديد الرئيسي الناجم عن الدعاوى القضائية جراء الاحتيال الذي طال المستهلكين. وقد تم تأسيس ممارسات قوية للحوكمة المؤسسية في تلك الشركة، رغم أن هذه الممارسات كانت تركز أكثر على العمليات التشغيلية العامة مع قليل من التركيز على نظم تقنية المعلومات وعملياتها التشغيلية.

لقد أصبحت قضايا الحوكمة المؤسسية ذات أهمية متزايدة في السنين الأولى من القرن الحالي عندما شهدت الولايات المتحدة سلسلة من الإخفاقات لكبرى الشركات والذي كان السبب الرئيسي لها بشكل عام هو الغش المحاسبي والاحتيال المالي. وكانت الشركة التي عُرفت بالسمعة السيئة في تلك الفترة هي شركة إنرون Enron التجارية. فقد كان الإخفاق المفاجئ وغير المتوقع لتلك الشركة ناتجاً عن الاحتيال المالي الذي تسبب في الزج بالعديد من المديرين التنفيذين للشركة في السجون. وقد عَجَّل هذا الإخفاق لشركة إنرون في إقرار قانون ساربينز أوكسلي SOX في الولايات المتحدة الأمريكية، وكذلك في إيجاد مطالب مماثلة في جميع أنحاء العالم. ستقدم الأجزاء التالية من هذه الوحدة لمحة عامة عن الضوابط الداخلية لقانون SOx والتشريعات القانونية للحوكمة.

تسلك المفاهيم العامة للحوكمة التي ناقشناها في الفصل الأول اتجاهاً مغايراً بعض الشيء عندما نقوم بتقديم مفاهيم ونظم تقنية المعلومات ووضعهما في مزيج واحد. فالعديد من المفاهيم العامة لدينا حول حوكمة الإدارة قد تأسست واكتملت نوعاً ما في النصف الأخير من القرن العشرين. فوُضعت معايير، وكذلك ممارسات العمل بين الإدارة والمدققين الخارجيين والهيئات التنظيمية.

بالإضافة إلى إعطاء لمحة عامة حول المفاهيم الخاصة بقانون SOx، فإن هذا الفصل سيقدم أيضاً عرضاً رفيع المستوى لقضايا حوكمة تقنية المعلومات، متضمناً ذلك قضايا المؤسسة التشريعية والأمنية والمخاطر المرتبطة بتقنية المعلومات. كما سيناقش هذا الفصل التهديدات الداخلية والخارجية التي تؤثر في عمليات حوكمة تقنية المعلومات المؤسسية، إضافة إلى بعض خصائص الحوكمة الفعالة لتقنية المعلومات في المؤسسة. ويستعرض هذا الفصل أيضاً كلاً من المفاهيم العامة والخاصة لحوكمة تقنية المعلومات التي تُطبق على كبار المديرين اليوم. وسيتم الرجوع إلى العديد من هذه المفاهيم لاحقاً ومناقشتها بمزيد من التفصيل في فصول أخرى.

قانون ساربينز أوكسلي SOx:

قانون SOx هو قانون أمريكي كان قد صدر عام ٢٠٠٢ لتحسين عمليات إعداد التقارير المالية والتدقيق والحوكمة المؤسسية في الشركات العامة. وقد كان لهذا القانون في البداية أثر كبير في الأعمال في الولايات المتحدة، أما الآن فقد تم الاعتراف به واعتماده في جميع أنحاء العالم. وعلى الرغم من أن قواعد التدقيق والرقابة الداخلية لهذا القانون قد أسهمت وبشكل مباشر في تغيير العديد من ممارسات التدقيق الخارجي والممارسات المالية الخاصة بتقنية المعلومات، فإنه كان لهذا القانون أثر كبير أيضاً في حوكمة تقنية المعلومات. إن الفهم العام لهذا القانون من خلال التركيز على البند ٤٠٤ والمتعلق بقواعد الرقابة المحاسبية الداخلية يعد مطلب معرفي رئيسي بالنسبة لجميع كبار المديرين.

لقد أصبح قانون SOx قانوناً أمريكياً استجابةً لسلسلة من المخالفات المحاسبية والإخفاقات المالية التي كانت قد تعرضت لها في السابق شركات كبرى كإنرون Enron وورلد كوم WorldCom. وقد تسبب قانون SOx في إحداث العديد من التغيرات

الرئيسية التي كانت قد أثرت في عمليات حوكمة الشركات والعمليات المحاسبية وعمليات تدقيق التقارير المالية -بداية في الولايات المتحدة وحالياً في جميع أنحاء العالم. وعلى الرغم من أن قانون SOx عبارة عن مجموعة شاملة من التشريعات التي تحتوي على العديد من المكونات، فإن الجزء الأعظم من اهتمام الأعمال والمدققين الخاضعين لهذا القانون قد انصب على البند ٤٠٤ منه والمتعلق بقواعد تصديق أو إقرار الخضوع للرقابة الداخلية. وقد تسببت هذه الإجراءات المتعلقة بتدقيق الرقابة الداخلية في بذل المزيد من الجهد والاهتمام عندما بدأت الشركات بإقرار الالتزام بقانون SOx. يقدم هذا القسم نظرة عامة رفيعة المستوى عن قانون SOx الموجود حالياً، مع التركيز أكثر على البند ٤٠٤ منه والقواعد الأكثر أهمية بالنسبة لقضايا حوكمة تقنية المعلومات. وسنلخص متطلبات هذا القانون الخاصة بمراجعات الضوابط المحاسبية الداخلية، كما سنلخص أحد معايير التدقيق الخارجي الذي يعتبر جديداً نسبياً والذي يطلق عليه معيار التدقيق رقم (Auditing Standard No. 5 (AS5 5، وهو مجموعة إضافية من طرق الرقابة القائمة على المخاطر والذي يؤكد أيضاً أهمية القيام بمراجعات للضوابط الداخلية للتقارير المالية. بناء على ما تقدم فإنه يجب أن يكون لدى جميع كبار المديرين في المؤسسة مستوى عام من المعرفة والفهم الخاصة بقواعد الرقابة الداخلية لقانون SOx(1).

العناصر الأساسية لحوكمة تقنية المعلومات الخاصة بقانون SOx:

إن الاسم الرسمي لقانون SOx هو قانون إصلاح المحاسبة العامة وحماية المستثمرين (Public Accounting Reform and Investor Protection Act). وقد أصبح قانوناً تشريعياً في شهر أغسطس عام ٢٠٠٢م، وتم إصدار معظم القواعد واللوائح التنظيمية التفصيلية النهائية لهذا القانون مع نهاية العام التالي. ولأن اسمه يبدو طويلاً بعض الشيء، فقد أطلق عليه رجال الأعمال اسم قانون ساربنز أوكسلي SOx نسبة لأسماء أعضاء الكونجرس الأمريكي الأساسيين الرعاة لهذا القانون. يشير أغلب المهنيين بشكل عام إلى هذا القانون باسم SOx، أو SOX، أو Sarbox، وذلك من بين العديد من الأسماء الأخرى.

لقد قدم قانون SOx مجموعة من العمليات المختلفة كلياً فيما يخص الرقابة الخارجية، كـما قام باسـناد العديد من المسـئوليات الجديدة للحوكمة إلى كبـار المديرين التنفيذيين وأعضاء مجلس الإدارة. كما تم بموجب هذا القانون إنشـاء مجلس الإشراف المحاسبي على الشركات المسـاهمة Public Company Accounting Oversight Board (PCAOB) وهـو الهيئة المسـؤولة عن وضع القوانـين، وهو خاضع لهيئـة الأوراق الماليـة والبورصة الأمريكيـة Securities and Exchange Commission (SEC) وهـي الهيئة التي تقوم بإصـدار المعايير الخاصة بالتدقيق المـالي والإشراف على حوكمة المدقق الخارجي. وكما هو الحال بالنسبة لجميع القوانين الاتحادية المتعلقة بالأموال والسندات المالية، فقد تم تطوير مجموعـة إضافيـة من اللوائح والقوانـين الإدارية من قبل هيئـة الأوراق المالية والبورصة الأمريكية وذلك استناداً إلى تشريعات SOx.

يتـم تنظيم وإصدار القوانين الاتحادية الأمريكية على شـكل أقسـام منفصلة بداخل القانون التشريعي تسـمى أبـواب، ويندرج تحت كل باب مجموعة مـن البنود المرقمة والبنود الفرعية. ويشتمل قانون SOx على العديد من القواعد التي ليست بتلك الأهمية الكبيرة بالنسبة للعديد من المهنيين. نذكر على سبيل المثال البند ٦٠٢ (د) من الباب الأول والتـي تنص على أنه يجـب على هيئة الأوراق المالية والبورصـة الأمريكية أن تضع الحد الأدنى من معايير أو قواعد السـلوك المهني الخاصة بالمحامين الممارسـين والتابعين للجنة مراقبـة عمليات البورصـة[*] . وقد يكون من الجيد أن نعرف أن هـذا الأمر ليس له أي تأثير يذكر في إدارة المؤسسـة وحوكمة تقنية المعلومات. يوجز الشكل التوضيحي (٢-١) الأبواب أو البنود الرئيسـية لقانون SOx، علما بأن تركيزنا سـيكون فقط على الباب الأول والرابـع من القانون. فلسـنا بصدد وصف جميع بنود قانـون SOx أو إعادة نشر النص الكامل لهذا التشريع الذي يمكن أن نجده على شـبكة الويب[٢]، وإنما نهدف إلى تسـليط الضوء على الأجزاء الأكثر أهمية بالنسبة للمهنيين المعنيين بهذا القانون. وسنبدأ بمناقشة الباب الأول من قانون SOx والخاص بمجلس الإشراف المحاسـبي على الشركات المساهمة PCAOB وقواعد البند ٤٠٤.

[*] وهي أحد بنود الباب السـادس، وتنص على وضع قيود تحد من ممارسـة المهنيين بصفة وسيط أو مستشار أو تاجر (المترجم).

شكل توضيحي (٢-١)

موجز الأحكام الرئيسية لقانون SOx.

البند	الموضوع	القاعدة أو الشرط المطلوب
١٠١	إنشاء مجلس الإشراف المحاسبي على الشركات المساهمة PCAOB.	القواعد العامة لإنشاء مجلس الإشراف المحاسبي على الشركات المساهمة PCAOB متضمنة متطلبات الحصول على عضوية المجلس.
١٠٤	مراقبة شركات المحاسبة	الجدول الزمني لعمليات التفتيش التي يقوم بها مجلس الإشراف المحاسبي على الشركات المساهمة PCAOB على شركات المحاسبة العامة المسجلة.
١٠٨	معايير التدقيق	سيقبل مجلس الإشراف المحاسبي على الشركات المساهمة PCAOB معايير التدقيق الحالية إلا أنه سيقوم بإصدار معايير جديدة له.
٢٠١	ممارسات خارج النطاق	تحدد الممارسات المحظورة على شركات المحاسبة كالاستعانة بمصدر خارجي لعملية التدقيق الداخلي (تعهيد التدقيق الداخلي)، أو مسك الدفاتر المحاسبية أو تصميم النظم المالية.
٢٠٣	تناوب شريك التدقيق	يجب تبديل المدقق الرئيسي والمدقق المراجع بشكل منتظم كل خمس سنوات.
٣٠١	استقلالية لجنة التدقيق	يجب على جميع أعضاء لجنة التدقيق أن يكونوا مديرين مستقلين.
٣٠٢	مسؤولية الشركات عن التقارير المالية.	يجب أن يصدق كل من الرئيس التنفيذي CEO والمدير المالي CFO شخصياً على جميع التقارير المالية الدورية.
٣٠٥	موانع خاصة بالموظفين والمديرين	إذا تم تلقي مقابل أو مكافأة كجزء من عملية احتيالية أو عملية محاسبية غير قانونية، فإن الموظف أو المدير المستفيد مطالب بإعادة الأموال التي تلقاها بشكل شخصي.
٤٠٤	تقارير الرقابة الداخلية	الإدارة هي المسؤولة عن التقييم السنوي للضوابط الداخلية.
٤٠٧	الخبير المالي	يجب أن يكون الخبير المالي أحد مديري لجنة التدقيق.

٤٠٨	تحسين مراجعة الإفصاحات المالية.	قد تقوم هيئة الأوراق المالية والبورصة الأمريكية بوضع إطار زمني لعدة مراجعات للمعلومات المالية المدونة بالتقارير استناداً إلى عوامل محددة.
٤٠٩	الإفصاح في الوقت الحقيقي	يجب أن توزع التقارير المالية بطريقة سريعة وفورية.
١١٠٥	محظورات الموظف أو المدير	قد تمنع هيئة الأوراق المالية والبورصة الأمريكية المدير أو الموظف من العمل في شركة عامة أخرى في حال كان مدان في إحدى المخالفات.

الباب الأول من قانون SOx: مجلس الإشراف المحاسبي على الشركات المساهمة PCAOB:

قـدم قانون SOx قواعد جديـدة وهامة للمدققين الخارجيـين. فقبل ظهور قانون SOx كان المعهد الأمريكي للمحاسـبين القانونيـين AICPA (American Institute of Certified Public Accountants) هو المسـؤول عن وضع الإرشادات لجميع المدققين الخارجيين وشركات المحاسبة العامة التي يعملون بها وذلك من خلال مسؤوليته الكاملة عن شـهادة المحاسب القانوني (CPA) Certified Public Accountant. وبينما قامت مجالس المحاسـبة في الولايات في الواقع باعتماد محاسـبين قانونيين CPAs، كان المعهد الأمريكي للمحاسـبين القانونيين هو السَـبَّاق في حمل كامل المسـؤولية الخاصة بالمهنة. كـما تم أيضاً وضع معايير التدقيق الخارجي من قِبل مجلس معايير التدقيق Auditing Standards Board (ASB) التابـع للمعهـد الأمريكي للمحاسـبين القانونيين AICPA. وعلى الرغم من أن المعايير الأساسـية - التي يطلق عليها اسـم معايير التدقيق المقبولة قبولاً عامـاً Generally Accepted Auditing Standards (GAAS) -كانت موجودة دائمـاً ومعمولاً بها على مر السـنين، إلا أن هناك معايير تدقيق أحـدث قد تم إصدارها على شـكل نشرات مرقمة عن معايير التدقيق Statements on Auditing Standards (SASs). لقد كان الكثير من معايير التدقيق المقبولة قبولاً عاماً GAAS مجرد ممارسات جيدة للتدقيق، مثل أنه يجب أن تكون المعاملات المحاسبية مدعومة بالوثائق اللازمة، في

حين تناولت النشرات المرقمة لمعايير التدقيق SASs مجالات معينة بحاجة إلى مزيد من التوضيــح أو التعريف. كالنشرة المعيارية رقم ٩٩ SAS No. 99 التي تناولت الاعتبارات المتعلقــة بالعمليات الاحتيالية في القوائم المالية. حيث تشــترط قواعد الســلوك المهني الخاصة بالمعهد الأمريكي للمحاســبين القانونيين وجود محاسبين قانونيين (CPAs) لاتباع جميع معايير التدقيق (القابلة للتنفيذ) والتوافق معها.

وقد قامت هيئة الأوراق المالية والبورصة الأمريكية بقبول معايير التدقيق المقبولة قبولاً عاماً والخاصة بالمعهد الأمريكي للمحاســبين القانونيين (AICPA's GAAS) ونشرات معايير التدقيــق SAS الخاصــة بها. وقد حددت قواعد التدقيق هــذه، معايير التدقيق الخارجي والاختبارات الضرورية التي يجب تطبيقها على القوائم المالية الخاضعة للتدقيق. من جهة أخرى، أشــارت الفضائح المحاســبية التي أدت إلى إصدار قانون SOx إلى أن عملية إنشــاء معايير التدقيق التي يقودها المعهد الأمريكي للمحاسبين القانونيين قد "عُطلت". وقد انتزع قانــون SOx عملية وضع معايير التدقيق هذه من المعهد الأمريكي للمحاســبين القانونيين والتي كانت خاضعة لهيمنة شركات المحاســبة العامة الكبرى، كما عمل القانون على إنشاء مجلس الإشراف المحاســبي على الشركات المساهمة، وهو مؤسسة غير اتحادية، وغير ربحية تقــع على عاتقها مســؤولية الإشراف على جميع عمليات التدقيــق الخاصة بالشركات التي تخضع لهيئة الأوراق المالية والبورصة الأمريكية.

إن مجلس الإشراف المحاســبي على الشركات المساهمة PCAOB ليس بديلاً عن المعهد الأمريــكي للمحاســبين القانونيين AICPA، ولكنه تولى المســؤولية عن ممارســات التدقيق الخارجي التي يقوم بها الأعضاء التابعون للمعهد الأمريكي للمحاســبين القانونيين. ولا يزال المعهد الأمريكي للمحاســبين القانونيين مســتمراً في إدارة اختبار المحاسب القانوني المعتمد CPA وشــهاداته التي تُمنــح تبعاً لكل ولاية، كما يقوم المعهد أيضــاً بوضع معايير التدقيق للمنظمات الأمريكية الخاصة غير الخاضعة لهيئة الأوراق المالية والبورصة الأمريكية. وبينما يحدد الباب الأول من قانون SOx ممارسات التدقيق الخاصة بمجلس الإشراف المحاسبي على الشركات المســاهمة التي يقوم بها المدققون الخارجيون، نجد أن القواعد الأخرى لعمليات التدقيــق وحوكمة الشركات قد أســهمت أيضاً في تغيير الكيفية التي ينســق بها المدققون

الداخليون أعمالهم مع المدققين الخارجيين. وعلى الرغم من أن الباب الأول من قانون SOx يحتــوي على العديد من القواعد الجديدة، قد تكون القواعد الثلاث الأكثر أهمية بالنســبة للعديد من كبار المديرين هي أن مجلس الإشراف المحاســبي على الشركات المساهمة حالياً هو من تقع على عاتقه المســئولية الرئيسية عن مراقبة شركات المحاسبة العامة، وهو الذي يقوم أيضاً بوضع القواعــد الخاصة بمعايير التدقيق الخارجي لهذه الشركات ، ويقوم كذلك بوضــع قواعــد معايير التدقيق كالاحتفاظ بــأوراق العمل. تصف الفقــرات التالية بإيجاز قواعد عملية التدقيق الخارجي تلك والواردة في الباب الأول من قانون SOx.

إدارة مجلس الإشراف المحاســبي على الشركات المساهمة PCAOB وتسجيل شركات المحاسبة العامة: يدار مجلس الإشراف المحاسبي على الشركات المساهمة من خلال مجلس مُعــين من قبــل هيئة الأوراق الماليــة والبورصة الأمريكية بعضويــة مشروطة غير خاضعة لهيمنــة مصالــح المحاســبين القانونيين CPA وشركات المحاســبة العامــة. ويكون مجلس الإشراف المحاســبي على الشركات المساهمة هو المســؤول عن الإشراف على جميع شركات المحاسبة العامة التي كانت تمارس عملها قبل إنشاء هيئة الأوراق المالية والبورصة الأمريكية وتنظيمها، كما أنه مسئول أيضاً عن وضع معايير التدقيق.

معايير التدقيق ومراقبة الجودة والاســتقلال: يمتلك مجلس الإشراف المحاســبي على الشركات المســاهمة ســلطة وضع معايير التدقيــق والتوثيق المتعلقة بهــا، وكذلك معايير مراقبة الجودة وأخلاقيات العمل في شركات المحاســبة العامة المسجلة. كما يعترف قانون SOx بمعايير التدقيق التي كانت قد صدرت في الســابق عن المعهد الأمريكي للمحاســبين القانونيــين، وقد أصدر هذا القانون حتى الآن عدداً محدوداً من المعايير الجديدة، كمعيار التدقيــق رقــم ٥ AS5 الخاص بمراجعة وتقييم الضوابــط الداخلية. وتوضح قواعد قانون SOx أيضــاً أنه يجب أن يتضمن تقييــم المدقق الخارجي وصف نقاط الضعف الجوهرية وكذلك جميع الأمور الخاصة بعدم الامتثال الجوهري التي تم الكشــف عنها. فالمدققون الخارجيــون مطالبون بتعديل فاعلية الضوابــط الداخلية. وغياب مثل هذا التوثيق يجب اعتباره أحد نقاط الضعف في الضوابط الداخلية.

الاحتفاظ بأوراق عمل التدقيق: أوراق العمل هي الوثائق التي أعدت بواسطة المدققين خلال عملية التدقيق. ووفقاً لمعيار التدقيق رقم ٣ AS3 الصادر عن مجلس الإشراف المحاسبي على الشركات المساهمة والخاص بوثائق التدقيق، فإنه يجب الاحتفاظ بأوراق العمل الخاصة بالتدقيق وغيرها من الوثائق الداعمة لفترة زمنية لا تقل عن سبع سنوات. وقد جاء هذا المطلب بالتأكيد رداً على حدث مؤسف كان قد وقع قبيل سقوط شركة إنرون ومن ثم سقوط آرثر أندرسون Arthur Andersen، وهو مكتب التدقيق الخارجي للشركة. فقد كانت شركة إنرون لا تزال تعمل، ولكنها تعاني بعض الضغوطات المالية عندما أعلنت هيئة الأوراق المالية والبورصة الأمريكية بأنها تنوي إجراء معاينة فعلية (لوثائق التدقيق). وعلى إثر ذلك قام (مدققو مكتب) آرثر أندرسون، المدقق الخارجي للشركة، باستخدام إحدى السياسات الداخلية للشركة لتبرير عملية إتلاف جميع بل معظم وثائق التدقيق الحالية الخاصة بالشركة. وكان هذا الحدث أحد العوامل المحفزة التي أدت إلى وجود هذه القاعدة في قانون SOx.

نطاق اختبار الضوابط الداخلية: تشترط مبادئ مجلس الإشراف المحاسبي على الشركات العامة وجود مدققين خارجيين يقومون بوصف نطاق كلٍّ من عمليات الاختبار ونتائجها. فقبل ظهور قانون SOx كان المدققون الخارجيون أحياناً يقومون باستخدام السياسات الداخلية للشركة لتبرير العديد من الاختبارات التي يجرونها على عينات صغيرة من العناصر، فقد جرت العادة بأن يقوموا بإجراء اختباراتهم على عينات صغيرة من الأشخاص بالرغم من وجود عدد كبير من الذين يمكن إخضاعهم لعمليات الاختبار. وعندما تظهر النتائج الإيجابية للاختبارات ولم تظهر أية مشكلات، فإنهم يقومون بتعميم تلك النتائج الخاصة بالاختبارات التي أجريت على العينة الصغيرة على جميع العناصر أو الأشخاص. أما الآن فيجب عليهم إعطاء مزيد من الاهتمام لكلٍ من نطاق ومعقولية إجراءات الاختبار لديهم، ويجب أن تصف الوثائق المساندة بوضوح نطاق ومدى أنشطة الاختبار.

الباب الرابع لقانون SOx's: الإفصاحات المالية المعززة والبند ٤٠٤:

تم تخصيص الباب الرابع من قانون SOx لمعالجة بعض المشاكل الخاصة بالإفصاح عن التقارير المالية، والتشديد على القواعد الخاصة بتضارب المصالح بالنسبة لموظفي ومديري

الشركة، وتفويــض الإدارة بتقييم الضوابط الداخلية، وإصدار مدونة قواعد الســلوك لكبار الموظفــين وغيرها من القضايــا. يوجد العديد من البنود في هذا البــاب، إلا أن البند الأكثر أهمية بالنسبة لمعظم كبار المديرين هو البند ٤٠٤ والذي يدور حول تقييم الإدارة للضوابط الداخلية. يشترط قانون SOx أن تحتوي جميع تقارير (10K)(*) السنوية على تقرير الضوابط الداخلية الذي ينص على مسئولية الإدارة عن إنشاء نظام مناسب للضوابط الداخلية والحفاظ عليه، وكذلك تقييم الإدارة لمدى فاعلية تلك الإجراءات الموضوعة للضوابط الداخلية، وذلك اعتباراً من تاريخ انتهاء السنة المالية. هذا ما يُعْرَف عموماً بقواعد البند ٤٠٤. ويتحمل كل مــن المدققين الداخليين ومدققي تقنية المعلومات والاستشــاريين الخارجيين وحتى الفريق الإداري - باســتثناء المدققين الخارجيين - المســئولية عن مراجعــة وتقييم فاعلية الضوابط الداخليــة لديهم، ثم يأتي بعد ذلك دور المدققين الخارجيين للتصديق على مدى كفاية تلك المراجعات للضوابط الداخلية التي تم بناؤها ومراقبتها من قبل الإدارة.

يتــم دعم عمليات المراجعة الخاصة بالبند ٤٠٤ من قبــل قواعد معيار التدقيق رقم ٥ AS5 والتي ستناقش لاحقاً في هذا الفصل، وهي تعد من الأمور الهامة وخصوصاً للمدققين الداخلين نظراً لأن هذه القواعد توضح أنه من الممكن للمدققين الخارجيين أن يقوموا بعمل المدققين الداخليين في مراجعاتهم للضوابط الداخلية.

تنــص قواعــد البند ٤٠٤ من قانون SOx على أن المؤسســة هي المســؤولة عن مراجعة وتوثيــق واختبار الضوابط المحاســبية الداخليــة لديها، مع تمرير نتائــج تلك المراجعات إلى المدققين الخارجيين للمؤسسة والمكلفين بمراجعة تلك الأعمال والتصديق عليها على أنها جزء من مهامهم المتعلقة بمراجعة القوائم المالية المعلن عنها. عندما تم ســن قانون SOx لأول مــرة، كانت عمليات المراجعة الواردة في البند ٤٠٤ هي نقطة الاهتمام الرئيســية بالنســبة للعديــد من المؤسســات نظراً لأن المدققيــين الخارجيين كانوا في الســابق يتبعون مجموعة تفصيلية للغاية من الإجراءات الخاصة بعملية تدقيق المحاســبة المالية التي تم تحديدها في معيار التدقيق رقم ٢ AS2 الخاص بمجلس الإشراف المحاسبي على الشركات المساهمة، وهو

(*) هــو تقرير تطلبه هيئة الأوراق المالية والبورصة الأمريكية من الشركات للتأكد من مدى التزامها، وهو عبارة عن تقرير مالي ســنوي يعد من قبل الشركة في نهاية كل ســنة مالية ويجب أن يكون مصدقاً من المحاســب القانوني الخاص بالشركة. (المترجم).

الأمر الذي يحتاج إلى نهج تفصيلي للمراجعة لا يسمح بأي أخطاء أو هفوات حتى لو كانت صغيرة. وقد تغيرت بعد ذلك قواعد التدقيق الواردة في البند ٤٠٤ مع صدور معيار التدقيق رقـم ٥ AS5 من مجلس الإشراف المحاسـبي على الشركات المسـاهمة في عام ٢٠٠٧، والذي يعد أحد أسـاليب التدقيق القائمة أكثر على المخاطر، كما يسـمح أيضاً للمدققين الخارجيين باستخدام أعمال المدققين الداخليين في إجراء التقييمات الخاصة بهم على نحو أفضل.

البند ٤٠٤ تقييمات الضوابط الداخلية:

كانـت الإدارة دائماً هي التي تتحمل المسـؤولية الكاملة عن تصميـم وتطبيق ضوابط الرقابة الداخلية على عمليات التشـغيل داخل المؤسسة. وعلى الرغم من أن معايير تكوين الضوابـط الداخلية الجيدة لم تكن دائماً محددة بشـكلٍ جيد في الماضي، إلا أنها بقيت أحد المفاهيم الرئيسية للإدارة. يشترط البند ٤٠٤ من قانون SOx القيام بإعداد تقرير سنوي عن الضوابط الداخلية، يشـتمل على عناصر المعلومات التالية، على أنها جزء من نموذج التقرير السنوي 10k الذي تم فرضه من قبل هيئة الأوراق المالية والبورصة الأمريكية.

- بيان رسمي من الإدارة يقر بمسئولية المؤسسة عن إنشاء وصيانة هيكل وإجراءات مناسبة للرقابة الداخلية الخاصة بالتقارير المالية.

- تقييـم لفاعليـة بنية وإجراءات الرقابة الداخلية للتقارير المالية في المؤسسـة، اعتباراً من نهاية آخر سنة مالية.

وبالاضافـة إلى ذلك، فإن مكتب التدقيـق الخارجي الذي قام بإصـدار التقرير الداعم للتدقيـق، مطالب هو الآخـر بمراجعة تقييم الإدارة للضوابط الماليـة الداخلية الخاصة بها والإفصاح عن النتائج. نستطيع القول ببساطة إن الإدارة مُطالبة بالإعلان عن جودة ضوابط الرقابـة الداخلية لديها، كما يجب على شركة المحاسـبة العامة أن تدقق أو تصادق على أن الإدارة قـد قامت فعلاً بتطوير تقرير عن الضوابط الداخليـة بالإضافة إلى عملها الطبيعي والخاص بتدقيق القوائم المالية. لقد جرت العادة بأن تكون الإدارة هي المسئولة عن إعداد تقاريرهـا المالية الدورية، ثم يأتي بعد ذلك دور المدققين الخارجيين الذين يقومون بتدقيق تلـك الأرقام المالية والتصديق على سـلامتها. فبموجب البنـد ٤٠٤ من قانون SOx تكون

الإدارة هي المسؤولة عن توثيق وفحص الضوابط المالية الداخلية لديها وكذلك الإفصاح عن مـدى كفاءتها. ثم يقوم المدققون الخارجيون بعد ذلـك بمراجعة المواد الداعمة التي نتج عنهـا هذا التقريـر الخاص بالضوابط المالية الداخلية للتأكيد على أن هذا التقرير ما هو إلا وصف دقيق لبيئة الرقابة الداخلية.

بالنسـبة لمدقق القوائم غير المالية وبالتأكيد بالنسـبة للعديد من كبار مسؤولي الأعمال التنفيذيـين، قد يبـدو ذلك مطلباً غامضـاً أو تافهاً بعض الشيء. حتـى إن بعض المدققين الداخليين المنشـغلين بالدرجـة الأولى في عمليات التدقيق التشـغيلية قد يتسـاءلون عن الفروقات البسيطة في هذه العملية. في جميع الأحوال، فإن تقارير التدقيق المتعلقة بحالة الضوابط الداخلية كانت نقطة خلاف مستمرة بين المدققين الخارجيين وهيئة الأوراق المالية والبورصـة الأمريكية وغيرها من الأطراف المعنية على الأقل منذ عام ١٩٧٤. وكان جزء كبير من المشكلة هو عدم وجود تعريف متفق عليه يوضح المقصود بالضوابط الداخلية.

يصـف إطار الرقابـة الداخلية الصادر عن لجنة المنظـمات الراعية Committee Of Sponsoring Organizations (COSO)، الذي سـتتم مناقشته في الفصل الرابع من هذا الكتـاب، المعيار المعتمد لفهـم الضوابط الداخلية. فبموجب البنـد ٤٠٤ من قانون SOx فإن الإدارة مطالبة بإعداد تقرير عن مدى ملاءمة ضوابطها الداخلية، مع تصديق المدققين الخارجيين على هذه التقارير التي أعدتها الإدارة عن الضوابط الداخلية.

وتخضع هذه العملية إلى رقابة داخلية أساسية كمثال على أهمية الفصل بين المهام، لأن الشـخص الذي يقوم بتطوير المعاملات لا ينبغي أن يكون هو الشـخص نفسه الذي يوافق عليهـا. وبموجب إجراءات البند ٤٠٤، فإن المؤسسـة هي التي تقـوم ببناء وتوثيق عمليات الرقابة الداخلية لديها، ثم تقوم بعد ذلك جهة مسـتقلة كالتدقيق الداخلي بمراجعة وفحص تلك الضوابط الداخلية، وأخـيراً يقوم المدققون الخارجيون بمراجعة تلك العملية والتصديق على مدى كفايتها. وسـوف تسـتند إجراءات التدقيق المالي الخاصـة بهم إلى تلك الضوابط الداخلية. إن هذه العملية الواردة في البند ٤٠٤ تقوم بتحسـين الأمور التي كانت موجودة في الأيام التي سبقت صدور قانون SOx عندما كان يقوم المدققون الخارجيون ببناء وتوثيق وتدقيق الضوابط الداخلية لديهم بشكل متكرر، وهذا يعد خللاً في الفصل بين المهام.

تحديد العمليات الرئيسية للبدء في مراجعة الإمتثال للبند ٤٠٤:

لكل مؤسسة مجموعة من العمليات الأساسية تتعلق بدوراتها المحاسبية والتي من الطبيعي أن تُؤخذ في الاعتبار، سواء كان ذلك بالاعتماد على نظم تقنية المعلومات أو على الإجراءات اليدوية التي يتم أداؤها بصورة منتظمة، وهذه العمليات هي:

- **دورة الإيرادات:** وهي عمليات متعلقة بالمبيعات أو الإيرادات الأخرى للمؤسسة.
- **دورة النفقات المباشرة:** هي عبارة عن نفقات المواد أو التكاليف المباشرة للإنتاج.
- **دورة النفقات غير المباشرة:** عبارة عن تكاليف التشغيل التي لا يمكن ربطها مباشرة بالأنشطة الإنتاجية ولكنها ضرورية لعمليات تشغيل الأعمال بشكل عام.
- **دورة الرواتب:** تشمل كل مستحقات العاملين.
- **دورة المخزون:** بالرغم من أن المخزون سيعتبر في نهاية المطاف كنفقات إنتاجية مباشرة، فإن هناك حاجة لعمليات زمنية للحفاظ على المخزون لحين دخوله في الإنتاج.
- **دورة الأصول الثابتة:** تحتاج الممتلكات والمعدات إلى عمليات محاسبية منفصلة، مثل (المحاسبة الدورية للإهلاك) بمرور الزمن.
- **دورة الضوابط العامة لتقنية المعلومات:** تشمل هذه المجموعة من العمليات ضوابط تقنية المعلومات العامة أو القابلة للتطبيق على جميع عمليات تشغيل تقنية المعلومات.

يعد تحديد تلك العمليات المؤسسية الرئيسية خطوة مبدئية نحو تحقيق الامتثال للبند ٤٠٤، لذلك يجب على المؤسسة أن توثق وتعي وتختبر كل تلك "العمليات الرئيسية". وبالنسبة للعديد من المؤسسات، فهذه هي النظم الرئيسية وعمليات تقنية المعلومات الداعمة لها التي تراجع سنوياً من خلال عمليات التدقيق الخارجي.

دور التدقيق الداخلي:

على الرغم من أن قانون SOx لم يعط مسؤوليات محددة لعمليات التدقيق الداخلي، فإنها تعد مصدراً هاماً لإتمام عمليات تقييم الضوابط الداخلية الواردة في البند ٤٠٤. بموجب قانون SOx، فإنه يوجد إدارة مستقلة ومنفصلة في المؤسسة – تكون إدارة التدقيق الداخلي

أو تدقيــق تقنية المعلومات غالباً – تقوم بمراجعة وتوثيــق الضوابط الداخلية التي تغطي العمليات الرئيســية، وتحدد نقاط الرقابة الرئيسية، وتقوم بعد ذلك باختبار هذه الضوابط المحــددة. ومن ثم تقوم عملية التدقيق الخارجي بمراجعة هذا العمل وتصادق على مدى كفايته. وبالنسبة للعديد من المؤسسات، يمكن اعتبار عملية تدقيق تقنية المعلومات بأنها أحد المصادر الرئيسية لإجراء تلك المراجعات الخاصة بالضوابط الداخلية بالنسبة للعمليات القائمة على التقنية.

يجــب أن تعمــل الإدارة الماليــة العليا ولجنــة التدقيق مع المدققــين الخارجيين للمؤسســة لتحديد المســؤوليات الخاصة بمراجعات الضوابــط الداخلية الخاصة بهم والــواردة في البند ٤٠٤. وتجري هذه المراجعات ســنوياً باســتخدام الوثائق التي تم إعدادها واختبارها في أول ســنة مالية، ثم تُحَدّث بعد ذلك ويعاد اختبارها في فترات لاحقــة. لذا يجب على جميع الأطراف تطويــر نهج فعال من حيث التكلفة لتحقيق متطلبات قانون SOx وتقييم تطبيقات وضوابط تقنية المعلومات لديهم.

يجــب تخطيط وإجــراء المراجعات الخاصة بالبند ٤٠٤ مــن قانون SOx على غرار العديد من المشــاريع الجديــدة في تقنية المعلومات، كما جاء في الفصل التاســع عشر الذي يدور حول دور التدقيق الداخلي في حوكمة تقنية المعلومات. الشكل التوضيحي (٢-٢) يوجز بعض اعتبارات التخطيط اللازمة لمراجعة الرقابة الداخلية الواردة في البند ٤٠٤ عــلى أن يتم تنفيذها من قبل المدققين الداخليين في المؤسســة، والذين بإمكانهم أن يلعبــوا دوراً أساســياً في مســاعدة الإدارة العليا على تحقيــق الامتثال مع ما ورد في البند ٤٠٤. نحن لا نهدف هنا إلى توفير إرشادات للتدقيق الداخلي بقدر ما نهدف إلى إعطــاء المدير الأول (الأعلى) فكرة عن تلك العمليات الخاصة بالتدقيق الداخلي لتقنية المعلومات.

شكل توضيحي (٢-٢)

اعتبارات التخطيط لمراجعة الضوابط الداخلية الواردة في البند ٤٠٤

١.	حدد حالة المراجعة – هل هذه هي الجولة الأولى من المراجعات الواردة في البند ٤٠٤ بالنسبة للمؤسسة وسيتم متابعتها في السنوات اللاحقة؟
٢.	إذا كانت هذه هي المراجعة الأولى (مراجعة جديدة) اتبع خطوات العمل اللازمة لفهم وتوثيق واختبار العمليات الرئيسية. خلاف ذلك، خطط للمراجعة في فترة لاحقة.
٣.	قم بمراجعة الوثائق التفصيلية للمراجعات السابقة للبند ٤٠٤ ، متضمناً ذلك خرائط تدفق الإجراءات، وفجوات الرقابة الداخلية التي تم تحديدها ومعالجتها، وكذلك الوثائق الشاملة لتخطيط المشروع والخاصة بالمراجعة السابقة.
٤.	قم بمراجعة أي من القواعد الصادرة عن مجلس الإشراف المحاسبي على الشركات المساهمة قد تم نشرها مؤخراً يمكن أن تغطي المراجعات الواردة بالبند ٤٠٤ وتتعلق بالتغيرات التي تطرأ على التدقيق، وقم بضبط إجراءات المراجعة بحيث تعكس تلك التغييرات.
٥.	قم بالاجتماع مع مكتب التدقيق الخارجي المسئول عن التصديقات الحالية للبند ٤٠٤ وقم بتحديد ما إذا كان هناك أي تغيرات في الوثائق وفلسفة الاختبار، مع التأكيد على قواعد معيار التدقيق رقم ٥ AS5، من تلك المراجعة السابقة.
٦.	ضع في الاعتبار أي تغييرات تنظيمية قد طرأت منذ المراجعة السابقة، متضمناً ذلك الاستحواذات أو العمليات الرئيسية لإعادة الهيكلة، وتعديل المدى الذي ستقوم المراجعة بتغطيته، إذا اقتضت الحاجة ذلك.
٧.	من خلال اللقاءات مع الإدارة العليا وإدارة تقنية المعلومات، حدد ما إذا كان هناك نظم وعمليات جديدة قد تم تنصيبها خلال الفترة الماضية، وإذا ما كانت هذه التغييرات الجديدة قد تم تدوينها في الوثائق المحدثة.
٨.	قم بمراجعة أي من نقاط الضعف الخاصة بالرقابة الداخلية قد تم تعريفها في المراجعات السابقة وقم بتقييم ما إذا كانت إجراءات تصحيح الرقابة الداخلية المدونة بالتقرير يتم العمل بها على أرض الواقع.
٩.	قم بتقييم حالة الوثيقة الحالية للبند ٤٠٤ وحدد مدى ضرورة إعداد وثيقة جديدة.
١٠.	على افتراض أن المراجعة السابقة للبند ٤٠٤ قد تمت من قبل التدقيق الداخلي، قم بتحديد العناصر المدربة وذوي المعرفة المناسبة والمتاحة لإجراء المراجعة القادمة.

١١.	قم بعمل مقابلات شـخصية مع جميع الأطراف التي شاركت في إجراء المراجعة السابقة للبند ٤٠٤ لتقييم أي دروس مستفادة، وقم بوضع خطط للاجراءات التصحيحية في المراجعة القادمة.
١٢.	استناداً إلى المناقشة التي تتم مع المدققين الخارجيين والإدارة العليا، قم بتحديد نطاق المعاملات الجوهرية للمراجعة القادمة.
١٣.	قـم بتحديد ما إذا كانت البرمجيات – إن وجدت - المسـتخدمة في المراجعة السـابقة لا تزال موجـودة، وقم بعمل أي تغيرات ضروريـة حتى يكون لديك الأدوات الكافية والجاهزة لإجراء المراجعة القادمة.
١٤.	قـم بإعداد خطة تفصيلية لمشروع المراجعة القادمة للبند ٤٠٤، في ظل وجود اعتبارات معينة لتنسيق أنشطة المراجعة لدى وحدات الأعمال في المؤسسة والمدققين الخارجيين.
١٥.	قم بإرسال الخطة للموافقة عليها من قبل الإدارة العليا.

قواعد معيار التدقيق رقم ٥ AS5 والتدقيق الداخلي:

بعـد فترة وجيـزة من إقرار قانـون SOx في الولايات المتحدة، أصـدر مجلس الإشراف المحاسـبي على الشركات المساهمة إرشـادات معيار التدقيق رقم ٢ AS2 والذي دعُي فيه المدققـون الخارجيون إلى اتباع أسـاليب محافظة وتفصيلية للغايـة في تدقيقاتهم للقوائم المالية. فقد شـدد معيـار التدقيق رقم ٢ AS2 على نهج التدقيـق التفصيلي (انظر في كل شيء)، وأصبحـت فواتير عملية التدقيق الخارجي أغلى بكثير مما كانت عليه في السـنوات الأولى لإصدار قانون SOx فضلاً عن ذلك، فقد كانت هناك شـكاوى متكررة من قبل قادة الصناعة وآخرين وكان هناك إجماع عام على أن معيار التدقيق رقم ٢ AS2 يحتاج إلى بعض التنقيحـات. وقد تم الاتفاق بين كل من هيئة الأوراق المالية والبورصة الأمريكية ومجلس الإشراف المحاسـبي على الشركات المسـاهمة على تنقيح معيـار التدقيق رقم ٢ AS2، وتم إصدار معيار التدقيق رقم ٥ في أواخر شهر مايو من عام ٢٠٠٧م.

معيار التدقيق رقم ٥ AS5 هو مجموعة من المعايير الخاصة بالمدققين الخارجيين الذين يقومون بمراجعة واعتماد القوائم المالية المنشورة. وتعتبر هذه القواعد مهمة أيضاً بالنسبة للمدققين الداخليين. يقدم معيار التدقيق رقم ٥ مجموعة من القواعد القائمة على المخاطر مع التركيز على كفاءة الضوابط الداخلية المعتمدة أكثر على أحداث وظروف المؤسسة. هذا

بالإضافة إلى أن معيار التدقيق رقم ٥ يدعو المدققين الخارجيين أن يأخذوا بعين الاعتبار جميع مراجعات التقارير المناسبة الخاصة بالتدقيق الداخلي أثناء مراجعاتهم المتعلقة بتدقيق القوائم المالية. حيث يسمح هذا المعيار للمدققين الخارجيين بأن يركزوا أكثر على قدرة الإدارة على إيجاد وتوثيق الضوابط الداخلية الرئيسية.

إن لقواعد معيار التدقيق رقم ٥ أهمية خاصة بالنسبة للمدققين الداخليين نظراً لإمكانية اعتماد المدققين الخارجيين على أعمال المدققين الداخليين في تقييماتهم وفقاً للبند ٤٠٤. لمعيار التدقيق رقم ٥ ثلاثة أهداف رئيسية هي:

١- **تركيز عمليات تدقيق الرقابة الداخلية على المسائل الأكثر أهمية:** يدعو معيار التدقيق رقم ٥ المدققين الخارجيين إلى أن يركزوا في مراجعاتهم على المجالات ذات المخاطر البالغة التي ستُعجز الرقابة الداخلية عن منع أو اكتشاف التقارير غير الواضحة في البيانات المالية. إن هذا النهج يدعو المدققين الخارجيين أن يركزوا على تحديد نقاط الضعف الجوهرية في الرقابة الداخلية أثناء مراجعاتهم قبل أن تتسبب في وقوع أخطاء جسيمة في البيانات المالية. ويشدد معيار التدقيق رقم ٥ أيضاً على أهمية تدقيق المجالات العالية المخاطر، مثل عملية إقفال نهاية الفترة للقوائم المالية والضوابط المُصَمَّمة لمنع الاحتيال من قبل الإدارة. وفي ذات الوقت يوفر هذا المعيار مجموعة واسعة من البدائل للمدققين الخارجيين لمعالجة المجالات المنخفضة المخاطر، كأن يكون ذلك عن طريق عرض أكثر وضوحاً لكيفية التدرج في توضيح طبيعة وتوقيت ومدى الاختبار اعتماداً على المخاطر، وكذلك كيف يتم تضمين المعرفة المتراكمة من عمليات التدقيق التي تمت في السنوات السابقة في تقييم المدققين للمخاطر. وأيضاً من المهم جداً بالنسبة للمدققين الداخليين، أن معيار التدقيق رقم٥ يسمح للمدققين الخارجيين باستخدام الأعمال التي تم تنفيذها من قبل المدققين الداخليين في المؤسسة عند الحاجة.

٢- **إزالة إجراءات التدقيق غير الضرورية لتحقيق المنافع المرجوة:** لا يشتمل معيار التدقيق رقم ٥ على المتطلبات التفصيلية التي كانت موجودة في معيار التدقيق رقم ٢ AS2 السابق لتقييم عملية التقييم الخاصة بالإدارة ولتوضيح أن عملية تدقيق الرقابة الداخلية لا تستلزم المشورة حول مدى كفاية وملاءمة عمليات الإدارة. على سبيل المثال،

يركـز معيـار التدقيق رقم٥ على أبعـاد المخاطر المترتبة على تعدد المواقع في المؤسسـة ويقلل من المتطلبات التي تسـتوجب على المدققين الخارجيين بأن يقوموا بمراجعة "جزء كبير" من عمليات التشـغيل أو الأوضاع المالية في المؤسسـة. هذا من شـأنه أن يسمح بتقليص أعمال التدقيق المالي.

٣- **توسـيع نطاق عملية التدقيق المالي بشـكل واضح لتتلائم مع حجم ومستوى التعقيد لأي مؤسسة:** لتقديم الإرشادات الخاصة بعمليات التدقيق في المؤسسات الأصغر حجماً والأقـل تعقيداً، يدعو معيار التدقيق رقم ٥ إلى ضبط عمليات تدقيق الضوابط الداخلية بحيث تتناسـب مع حجـم ودرجة تعقيد المؤسسـة التي يتم تدقيقهـا. فلهذا المعيار إرشـادات تتعلق بالكيفية التي يتم فيها تطبيق معيار التدقيق رقم ٥ على المؤسسـات الأصغر حجماً والأقل تعقيداً وكذلك على وحدات المؤسسات الأكبر حجماً.

عقب إصدار معيار التدقيق رقم ٥ ، قد يفكر المدققون الخارجيون في مسـألة استخدام أعمال الآخرين للمسـاعدة في إتمام تدقيق الضوابط الداخليـة للقوائم المالية طبقاً لقانون SOx. وعلى الرغم من أن ذلك الأمر لم يكن واضحاً كما يجب وفقاً لقواعد معيار التدقيق رقم ٢ AS2 لقانون SOx، فإن معيار التدقيق رقم ٥ قد سـمح بذلك الآن بشـكل صريح. ينص معيار التدقيق رقم ٥ على أنه بإمكان المدقق الخارجي أن يسـتخدم الأعمال المنجزة بواسـطة، أو أن يتلقى مسـاعدة مباشرة من، المدققين الداخليـين أو الموظفين الآخرين في الشركـة أو الأطـراف الخارجية التي تعمل تحـت إشراف الإدارة أو لجنـة التدقيق، وذلك لتقديـم الأدلة الكافية على فاعلية الضوابط الداخلية للتقارير المالية. وقد كان ذلك تغييراً جوهرياً بالنسبة للمدققين الداخليين.

مـن المؤكد أن المدققين الخارجيين هـم من يقومون بالتوقيـع أو التصديق على نتائج التدقيق، ويجب عليهم أيضاً تقدير مدى كفاءة وموضوعية الأشـخاص الذين يتم التخطيط لاسـتخدام أعمالهم من قبل المدققين الخارجيين. فكلـما زادت درجة الكفاءة والموضوعية لدى هؤلاء الأشـخاص، زاد حجم الاسـتخدام الذي يمكن أن يفعله المدقق بأعمالهم. على وجه التحديد، يدعو معيـار التدقيق رقم٥ إلى تقييم كفاءة وموضوعية المدققين الداخليين في المؤسسـة. الكفاءة هنا تعني تحقيق (والحفاظ على) مستوى معين من الفهم والمعرفة

بما يُمَكِّن الأشـخاص مـن أداء المهام الموكلة إليهم، أما الموضوعيـة فتعني المقدرة على أداء تلـك المهام بنزاهة وأمانة معرفية. ولتقييم الكفاءة يتعـين على المدقق الخارجي أن يقوم بتقييـم مؤهلات المدققـين الداخليين أو غيرهم وقدرتهم على إنجـاز الأعمال التي يخطط المدقق الخارجي لاستخدامها. ولتقييم الموضوعية، فإن معيار التدقيق رقم ٥ يدعو المدقق الخارجي إلى تقييم ما إذا كانت العوامل الحالية تعرقل أو تعزز من قدرة الشخص على أداء الأعمال، بالقدر اللازم من الموضوعية، والتي يخطط المدقق (الخارجي) لاستخدامها.

يواصل معيار التدقيق رقم ٥ في النص على أنه لا يجب على المدققين الخارجيين استخدام أعـمال أشـخاص (هم) على "درجـة منخفضة مـن الموضوعية، بغض النظر عن مسـتوى كفاءتهـم"، كما لا يجب عليهم أيضاً اسـتخدام أعمال أشـخاص (هم) على درجة منخفضة مـن الكفاءة، بغض النظر عـن درجة موضوعيتهم. إن الأشـخاص الذين يضطلعون بمهام رئيسية كسـلطة الاختبار أو الامتثال في المؤسسة، مثل المدققين الداخليين أو مدققي تقنية المعلومات، هم عادة من يُتَوَقع أن يكونوا على درجة عالية من الكفاءة والموضوعية في أداء مثل هذا النوع من الأعمال التي ستكون مفيدة للمدقق الخارجي.

قواعد أخرى لقانون SOX — الباب الثاني: استقلالية المدقق:

كان المدققون الداخليون والخارجيون دائماً عبارة عن موارد منفصلة ومستقلة. فقد كان المدققون الخارجيون مسؤولين عن تقييم نزاهة أنظمة الرقابة الداخلية في المؤسسة والتقارير المالية المعلنة في النهاية. في حين كان المدققون الداخليون يخدمون الإدارة في مجموعة واسعة من المجالات الأخرى. في بدايات التسعينيات من القرن الماضي، بدأ هذا الانقسام بالتغير مع تحمـل شركات التدقيق الخارجي كامل المسـئولية تجاه بعض مهام التدقيق الداخلي أيضاً. وقد بدأ ذلك عندما شرعت المؤسسـات الكبيرة في الاستعانة بـمصادر خارجية للقيام ببعض الوظائف غير الأساسـية لديها كوظيفة عامل الكفتيريا أو عمال الخدمات المعاونة كالنظافة والحراسة وصيانة المعدات. كان التفكير وقتها في أن الموظفين الذين عملوا في تلك المجالات المتخصصة لم يكونوا في الواقع جزءاً من عمليات التشغيل الرئيسية في المؤسسة، وأن وظيفة الخدمات المعاونة وغيرها من الوظائف غير الرئيسية الخاصة بالمؤسسة ربما يتم إسنادها إلى شركات أخرى متخصصة في مجالات مثل تقديم الخدمات المعاونة إلى العديد من المؤسسات

الأخرى. وأن موظفي الخدمات المعاونة الذين كانوا يعملون سـابقاً داخل المنشـأة سـيتم تحويلهم إلى شركات تعمل في مجال الخدمات المعاونة، ونظرياً، فإن الكل سيسـتفيد. وإن المؤسسة التي بادرت بالاستعانة بالمصادر الخارجية ستتحمل تكاليف أقل، وذلك من خلال إسناد الوظيفة غير الرئيسية، وهي الخدمات المعاونة، إلى شخص ما أكثر تخصصاً فيها. وقد يكون لدى عامل الخدمات المعاونة الذي تم الاستعانة به على أنه مصدر خارجي احتمالات مهنية واعدة وإشرافية أفضل.

بدأت عملية الاستعانة بمصادر خارجية للقيام بمهمة التدقيق الداخلي لأول مرة في أواخر الثمانينيات من القرن الماضي. فقد لجأت مكاتب التدقيق الخارجي إلى إدارات الشركات التي تتولى مهام التدقيق الخارجي لديها وعرضت عليهم فكرة "الاستعانة بمصادر خارجية" أو أن تقوم الشركة بتولي المهام الحالية للتدقيق الداخلي. وقد نالت هذه الفكرة استحسان الإدارة العليا ولجان التدقيق على مختلف المستويات. حيث كانت الإدارة العليا في أغلب الأحيان غـير مدركة تماماً للفروقات الموجودة ما بين مهام عملية التدقيق الخارجي والداخلي وكانوا في بعض الأحيان يميلون أكثر للتعامل مع مدققيهم الخارجيين. هذا بالإضافة إلى أن الإدارة العليـا وأعضاء لجنة التدقيق كان يتـم إغراؤهم غالباً عن طريق وعود بانخفاض التكاليف في حال الاسـتعانة بمصـادر خارجية للقيام بعملية التدقيق الداخلي. وقد اسـتمر إسـناد التدقيـق الداخلي لمصادر خارجية (التعهيد بالتدقيق الداخلي) في النمو خلال تسـعينيات القـرن المـاضي. وبالرغم من المحاولات المبذولة من بعض الشركات المسـتقلة لدخول هذا السـوق، فإن إسناد التدقيق الداخلي لمصادر خارجية استمر ليكون المجال الخاص بشركات المحاسبة العامة الكبرى.

أصبحت الاستعانة بمصادر خارجية للتدقيق الداخلي مسألة بالغة الأهمية نظراً لضلوعه في فضيحة إنرون، فقد قامت الشركة بتعهيد مهام التدقيق الداخلي لديها بشـكل شبه كلي إلى مكتب التدقيق الخارجي الخاص بها، وهو مكتب آرثر أندرسون Aruther Andersen. حيث إن فريقي التدقيق، كلاهما يعمل بشكل رسمي بصفة موظف في مكتب أندرسون مع اختـلاف العلاقات الخاصة بإعداد وتقديم التقارير، فهم يعملون جنباً إلى جنب في مكاتب شركة إنرون. وعلى إثر سقوط شركة إنرون، ثارت العديد من التساؤلات عقب تلك الواقعة

عن كيف يمكن لإدارة التدقيق الداخلي تلك والتي تم التعهيد بها أن تكون إدارة مستقلة عن مكتب أندرسون. لقد كان من الصعب جداً في هذه الظروف التي يمر بها التدقيق الداخلي أن تُثار المخاوف لدى لجنة التدقيق المتعلقة بمدققيهم الخارجيين. وقد أصبح هذا التضارب المحتمل بمثابة قضية إصلاحية في قانون SOx.

القيود المفروضة على خدمات المدققين الخارجيين:

نص قانون SOx على أنه من غير القانوني بالنسبة لأي شركة من شركات المحاسبة القانونية (العامة) المسجلة أن تقوم بتقديم خدمات غير متعلقة بالتدقيق بالتزامن مع تقديم خدمات التدقيق لنفس العميل. تشمل هذه المحظورات أعمال التدقيق الداخلي، والعديد من مجالات الاستشارات، والتخطيط المالي لمسئول كبير. والعنصر الأكثر أهمية هنا هو أنه من غير القانوني بالنسبة لشركات المحاسبة القانونية أن تقوم بتقديم خدمات التعهيد الخارجي لأعمال التدقيق الداخلي في حال كانت هي أيضاً من يقوم بأعمال التدقيق. هذا يعني أن شركات المحاسبة القانونية الكبرى قد تكون حالياً وبشكل أساسي خارج نطاق التعهيد الخارجي لأعمال التدقيق الداخلي بالنسبة لعملاء التدقيق المباشرين لديها. أما الشركات الأخرى، متضمناً الشركات المستقلة المنفصلة عن شركات مستوى المحاسبة العامة أو الشركات الاستشارية المتخصصة في التدقيق الداخلي يمكنهم الاستمرار في تقديم خدمات التعهيد الخارجي لأعمال التدقيق الداخلي. أما العصر الذي كان فيه من الممكن أن يصبح أحد أخصائيي التدقيق الداخلي متعاقداً أو موظفاً في شركة المحاسبة العامة الخاصة به أو بها قد انتهى.

إضافة إلى الحظر المفروض على تقديم خدمات التعهيد الخارجي لأعمال التدقيق الداخلي، فإن قانون SOx يمنع مكاتب المحاسبة القانونية من تقديم خدمات أخرى منها:

- **تصميم نظم المعلومات المالية وتطبيقاتها:** كانت مكاتب المحاسبة القانونية ولسنوات عديدة تقوم بتثبيت نظم مالية – تكون غالباً من تصميمها الخاص – لعملائها من الشركات. ثم يعودون بعد ذلك لمراجعة الضوابط الداخلية لتلك النظم التي قاموا للتو بتركيبها – ويعد هذا تضارباً كبيراً في المصالح، ولم يعد هذا مسموحاً به.

- **مسـك الدفـتر والخدمات المتعلقة بالقوائـم المالية:** كانت مكاتب المحاسـبة العامة في السـابق تقوم بتقديم خدمات محاسـبية لعملائها بالإضافة إلى قيامهـا بأعمال التدقيق وحتى بالنسـبة للشركات الكبرى، فلم يكن من غير المعتاد بالنسـبة للفريق المسئول عن عملية تدقيق القوائم المالية بالكامل أن يقوم أيضاً بإجراء الكثير من الأعمال اللازمة لبناء القوائم المالية الموحدة (المجمعة) النهائية. مرةً أخرى يعد هذا تضارباً محتملاً في المصالح، وهذا غير مسموح به.

- **الوظائف الإدارية ووظائف الموارد البشرية:** قبل صدور قانون SOx، كانت مكاتب التدقيق الخارجي هي التي تقوم غالباً باختيار عدد من المهنيين العاملين لديها وتسـاعد في انتقالهم إلى مناصب إدارية لدى العميل. وكانت النتيجة إيجاد بيئة يكون فيها كل مديري الحسابات تقريباً في المؤسسـة هم مـن خريجي مكتب التدقيق الخارجي التابعـين له. وقد كان ذلك محبطـاً أحياناً بالنسـبة للمدققين الداخليين وغيرهم من الذين لا ينتمون لمكتب المحاسـبة القانونية نفسه . وبدت فرص الحصول على ترقية فوق مستوى معين محدودة بسبب شبكة علاقات أو اتصالات "التلميذ السابق"(*) Old-boy مع مكتب التدقيق الخارجي.

- **خدمـات أخرى محظورة:** يَمنع قانون SOx مكاتب التدقيق الخارجي بصورة خاصة من تقديم الخدمات الاكتوارية (المتعلقة بحسـابات التأمين) والخدمات الاستشارية المتعلقة بالاسـتثمار والخدمات القانونية ذات الصلة بتدقيق الحسـابات. بالرغم من السماح لهم بتقديم الخدمات الضريبية.

إن الموضوع العام لقانون SOx هنا هو أن المدققين الخارجيين مخولون لمراجعة القوائم الماليـة الخاصة بعملائهم من المؤسسـات، وهذا كل ما في الموضوع. يسـمح قانون SOx بتجاوز الأنشـطة المحظـورة التي تم ذكرها، حيث يمكن للمدققين الخارجيين المشـاركة في تقديم الخدمات الأخرى غير المتعلقة بالتدقيق فحسب إذا كانت هناك موافقة مسبقة من قبـل لجنة التدقيق عـلى تقديم تلك الخدمات. فمع الفحوصـات المتزايدة التي تقوم بها لجان التدقيق في ظل قانون SOx، أصبح العديد يشعرون بالقلق جراء محاولة مصادقة أي شيء يبدو أنه خارج عن المألوف إطلاقاً.

(*) العلاقات والروابط الاجتماعية والتجارية بين التلاميذ السابقين. (المترجم).

الموافقة المسبقة من لجنة التدقيق على الخدمات:

يوضح البند ٢٠٢ من الباب الأول لقانون SOx أنه يجب أن توافق لجنة التدقيق على جميع الخدمات المتعلقة وغير المتعلقة بالتدقيق بشكل مسبق. وعلى الرغم من أن لجان التدقيق كانت تفعل أو كان يجب عليها أن تفعل ذلك طيلة الوقت، فإن تلك التصديقات أو الموافقات كانت في كثير من الأحيان أكثر بقليل من مجرد إجراء شكلي، وذلك قبل صدور قانون SOx. فقد كانت لجان التدقيق في شبكة "التلاميذ السابقين" Old -Boys تتلقي غالباً ما هو أكثر قليلاً من مجرد مذكرة مختصرة مكتوبة أو رسالة شفوية من الإدارة المسؤولة عن التدقيق والتي كانت تُعْتَمَد بالطريقة التقليدية نفسها التي كانت تُعْتَمَد بها في كثير من الأحيان محاضر الاجتماعات. وجاء قانون SOx ليغير كل هذا، فالآن قد يُعرِّض أعضاء لجنة التدقيق أنفسهم للمساءلة القانونية أو إقامة دعاوى قضائية ضدهم من قبل أصحاب المصالح في حال سماحهم بحدوث أي عمل من الأعمال المحظورة.

بالطبع فإن هناك العديد من الأمور الثانوية المتعلقة بأنشطة المدققين الخارجيين التي ليس من الضروري أن تمر من خلال تلك العملية الرسمية والخاصة بالموافقة المسبقة من قبل لجنة التدقيق.

وباستخدام المصطلحات القانونية، فإن قانون SOx يضع الحد الأدنى لقواعد الاستثناء[٣] من متطلبات الحصول على إذن لجنة التدقيق. فوفقاً لقانون SOx فإن الموافقة المسبقة ليست ضرورية بالنسبة لبعض الخدمات التي لا تتعلق بالتدقيق إذا كان:

- القيمة الإجمالية بالدولار الأمريكي للخدمة المقدمة لا تتجاوز ٥٪ من إجمالي رسوم عملية التدقيق الخارجي المدفوعة من قبل الشركة خلال السنة المالية التي قدمت فيها تلك الخدمات.
- كانت الخدمات المقدمة غير متعارف على أنها خدمات تتعلق بالتدقيق من قبل الشركة في الوقت الذي بدأت فيه عملية التدقيق الشامل.
- إذا حوِّلت هذه الخدمات لعناية لجنة التدقيق وتم الموافقة عليها قبل إتمام عملية التدقيق.

قَدَّمت تلك الاستثناءات بعض المرونة للمدققين الخارجيين ولجنة التدقيق. فضلاً عن أن طبيعة ومجموع القيمــة الدولارية لهذه الخدمات الإضافية التي لا تتعلق بالتدقيق يجب متابعتها بعناية طوال السنة المالية للحفاظ على مستوى معين من الامتثال. ولا بد من إشراك التدقيــق الداخلي في هذه العملية للمســاعدة في التأكد مــن أن جميع الخدمات الإضافية المقدمــة لا تزال متوافقة مع قواعد قانون SOx، متضمناً ذلك الإفصاح عنها للمســتثمرين عن طريق البيان الســنوي للوكيل. ويسمح SOx بإمكانية أن تقوم لجنة التدقيق بتفويض ســلطة الموافقة المسبقة على الخدمات التي لا تتعلق بالتدقيق لواحد أو أكثر من المديرين الخارجيين في لجنة التدقيق. وهذا من شأنه تخفيف الإجهاد الناتج عن الإجراءات المطولة للجنة التدقيق، ولكنه ســيضع مسؤولية أكبر على عاتق عدد قليل من أعضاء لجنة التدقيق علاوة على العديد من المسؤوليات القانونية الجديدة المفروضة من قبل قانون SOx.

تناوب شريك التدقيق الخارجي:

صرح بنــد آخــر (البند ٢٠٣) من الباب الثاني لقانون SOx أنه من غير القانوني أن يرأس الشريك الرئيسي لمكتب المحاســبة القانونية أية اتفاقيات لأكثر من خمس ســنوات. وهي المسألة التي قامت مكاتب المحاسبة الكبرى بتصحيحها بشكل جيد قبل صدور قانون SOx. فقد كان يتم تناوب الشركاء الرئيسيين التابعين للشركات الكبرى بصفة منتظمة، على الرغم من أنه قد تكون هناك اســتثناءات بالنســبة للشركات الصغرى واتفاقيات الشراكة الأصغر حجماً. وفي الوقت الذي شاعت فيه عملية تناوب الشريك الرئيسي، فقد اعتبر قانون SOx أن تقصير الشركة في عملية التناوب يعد عملاً إجرامياً. فضلاً عن أن، قانون SOx في الواقع لم يتناول ممارســة عامة يتم من خلالها تناوب شريك التدقيق حيث ســيقوم شخص معين بلعــب دور الرئيــس أو الشريك الرئيسي لعملية التدقيق، ثم يســتمر بعد ذلك في الخدمة كاستشــاري بعد انتهاء مدته أو مدتها. ويمكن لهذا الشريك الذي يلعب دور الاستشــاري غالباً أن يحافظ على مســتوى المسئولية نفسه المعين عليه الشريك الرئيسي وقد يصبح ذلك انتهاكاً محتملاً لقواعد قانون SOx.

عند طباعة هذا الكتاب كانت هناك العديد من الشــائعات والأقاويل التي تشير إلى أن مجلس الإشراف المحاســبي على الشركات المســاهمة PCAOB يقوم بدراسة فرض تناوب

كامل لمكاتب المحاسـبة القانونية (ليس تناوب شريكها). ففي الوقت الحالي قد يتم تبديل الـشركاء ولكن يبقي المكتب دون تغيير. التفكير في أن يكون هناك مكتب جديد يمد إدارة المؤسسة بمنظور جديد حول عملية التدقيق.

يتواصـل المدققون الخارجيون دائماً مع لجان التدقيق التابعين لها بصفة منتظمة طوال عملية التدقيق، وكذلك في حالة المسائل التي تثير المخاوف. وفي أعقاب سقوط شركة إنرون وغيرها من فضائح الشركات في ذلك الوقت، تم اكتشاف أن هذه الاتصالات كانت في بعض الأحيان محدودة للغاية. فقد يتفاوض أحد أعضاء الإدارة مع شريك المحاسبة القانونية على "التغاضي عن" تغيير مقترح في إحدى المعالجات المحاسبية، إلا أن لجنة التدقيق لم تكن تُبَلَّغ بهذا الأمر إلا في ظل الشروط العامة، وهذا في حال حدوث ذلك.

لقد غير قانون SOx ذلك. فالمدققون الخارجيون مطالبون بالإبلاغ -على أسـاس زمني- عن كل السياسات والممارسات المحاسبية المستخدمة، والمعالجات البديلة للمعلومات المالية التي تمت مناقشـتها مع الإدارة، والمعالجات البديلة الممكنـة، والنهج الذي يفضله المدقق الخارجـي. فالفكرة كلها هنا هي أنه يجب على المدققين الخارجيين أن يقوموا بإبلاغ لجنة التدقيق التابعين لها بأي معالجات محاسبية بديلة، والنهج المفضل لدى المدققين الخارجيين، ونهج الإدارة. هذا في الواقع يقول إنه إذا كانت هناك معالجات محاسـبية مختلف عليها، فإنه يجب أن تكون لجنة التدقيق على دراية جيدة بالإجراءات المتخذة حيال ذلك. ويشير هذا المطلب حقيقة إلى الحاجة إلى توثيق جيد للجنة التدقيق.

تضارب المصالح والتناوب الإلزامي لمكاتب التدقيق الخارجي:

لقد كان شـائعاً في السـابق بالنسـبة لأعضاء فريق مكتب التدقيق الخارجي أن يحصلوا على تعيينات وظيفية لشـغل مراكز مالية عليا لدى الشركات العميلة لديهم. وقـد منـع البند ٢٠٦ من الباب الثـاني لقانون SOx المدققـين الخارجيين من تقديم أي خدمات تتعلق بالتدقيق للشركة التي شـارك رئيسـها التنفيذي CEO أو مديرها المـالي CFO أو مدير حسـاباتها باعتباره أحد أعضاء مكتـب التدقيق الخارجي على عملية التدقيق نفسـها خلال السنة الأخيرة. وفي الحقيقة فإن هذا يعني أنه لا يمكن لشريـك عملية التدقيق أن يتخلى عن العمل في التدقيـق ليبدأ العمل مديراً تنفيذياً

في الشركة نفسـها التي قام للتو بتدقيق حسـاباتها. في حين أن الموظفين والمديرين لا يـزال بإمكانهم الانتقال من فريق مكتب المحاسـبة القانونية لتولي مناصب مختلفة في الشركـة الخاضعة لعملية التدقيق، فهذا الحظر يقتصر فقط على شركاء المحاسـبة القانونيـة وقد كانت هناك بعض الأمثلة الواضحة على هذا التحول في الأدوار باعتبار ذلك جزءاً من مجمل الأحداث الخاصة بشركة إنرون.

الباب الثالث لقانون SOx: مسؤولية الشركة:

تحتـوي اللوائح في البـاب الثالث من قانون SOx على قواعد تنظيمية رئيسـية تتعلق بلجـان التدقيق وتصـف معايير أداء لجـان التدقيق ومجموعة كبيرة مـن قواعد حوكمة الشركات. فبموجب قانون SOx، يجب على جميع المؤسسات المسجلة أن يكون لديها لجنة تدقيق مكونة فقط من مديرين مسـتقلين. حيث يتبع مدققـو مكتب التدقيق الخارجي لجنة التدقيق بشكل مباشر والمسئولة عن دفع أتعابهم والإشراف على أعمال التدقيق، وحل أي خلافات تقع بين التدقيق الخارجي والإدارة. وبالرغم من أن الشركات الأمريكية الكبرى قد كان لديها لجان تدقيق، فإن هذه القواعد قد تم اسـتنتاجها من الممارسـات التقليدية القديمـة. على سـبيل المثال، بينما كان لدى إدارات التدقيق الداخلي في السـنوات الماضية علاقـات ضعيفة خاصة بتقديم التقارير مع لجان التدقيق التابعين لها في كثير من الأحيان، فإن قانون SOx جعل هذه العلاقة أكثر قوة وأكثر فاعلية.

يجب أن يكـون كل عضو من أعضاء لجنة التدقيق التابعـة للمجلس (مجلس الإدارة) مديراً مستقلاً تماماً. ويجب أن يكون عضو واحد على الأقل من أعضاء لجنة التدقيق "خبيراً مالياً". وقد تم طرح هذه القوانين نتيجة جلسـات الاسـتماع التـي أدت إلى صدور قانون SOx، فقد تم اكتشاف أنه طُلب من بعض أعضاء لجنة التدقيق المسؤولة عن شركة إنرون الذيـن كانوا على ما يبدو لا يعرفون الكثير عن المعامـلات المالية القيام بعمليات المراجعة والاعتـماد. وتُعَرِّف اللوائح التنظيميـة لهيئة الأوراق المالية، والبورصـة الأمريكية "الخبير المالي" على أنه الشخص الذي يملك، من خلال التعليم والخبرة، التالي:

- فهم وإدراك للمبادئ المحاسبية والقوائم المالية المتعارف عليها بشكل عام.

- خبرة في تطبيق هذه المبادئ المحاسبية المقبولة بشكل عام وربطها بمحاسبة التقديرات والمستحقات والاحتياطات التي يمكن مقارنتها عموماً بالتقديرات والمستحقات والاحتياطات في حال استخدم أي منها في القوائم المالية للشركة المسجلة.

- خبرة في إعداد أو تدقيق البيانات المالية التي تمثل القضايا المحاسبية الحالية التي يمكن مقارنتها عموماً بتلك القضايا المحاسبية المثارة في القوائم المالية لدى الشركة المسجلة.

- خبرة في الضوابط والإجراءات الداخلية الخاصة بالتقارير المالية.

- فهم وإدراك لمهام لجنة التدقيق.

ولا تتطلب هذه المبادئ أي شهادات رسمية أو خلفيات أكاديمية أو مؤهلات أخرى. فهي تنص على أنه يجب على أعضاء لجنة التدقيق أن يقدموا أنفسهم على أنهم على مستوى معين من المعرفة حول قضايا المحاسبة والتقارير المالية والضوابط الداخلية. ففي بعض الأحيان يُطلب من عضو لجنة التدقيق أن يضع نفسه أو تضع نفسها في خط المواجهة في حال كانت المؤسسة يتم استجوابها دائماً فيما يخص بعض القرارات الخاصة بالمسائل المالية والرقابة الداخلية.

ويدعو قانون SOx أيضاً لجان التدقيق إلى أن تقوم بوضع إجراءات لتلقي وحفظ ومعالجة الشكاوى المقدمة ومعالجة إفادات المبلغين المتعلقة بالقضايا المحاسبية ومسائل التدقيق المشكوك فيها. هذا في الحقيقة يعني أن لجنة التدقيق يجب أن تصبح، في الواقع، كياناً مستمراً شبه مستقل، بدلاً من أن تكون مجموعة فرعية من المجلس الإداري التقليدي الذي يلتقي في مكان ما ويجتمع كل ثلاثة أشهر. وبينما هذا الأمر يبدو فكرة جيدة، فإن معظم وظائف لجنة التدقيق لا تملك مصادر داعمة لخدمة إدارة المبلغين على المستوى المؤسسي، ويكون هذا الأمر غالباً من اختصاص إدارة أخلاقيات العمل على المستوى المؤسسي. وعلى الرغم من النصوص الموجودة في قانون SOx، فإنه يتم تشغيل الإدارات الخاصة بالمبلغين على مستوى لجنة التدقيق في الأساس بحسب الظروف.

كانت الشركات الامريكية قبل صدور قانون SOx تقوم بحفظ قوائمها المالية داخل ملفات لدى هيئة الأوراق المالية والبورصة الأمريكية، ولكن لم يكن مديرو الشركات

المســؤولون الذين وقعوا على هذه التقارير المالية يتحملون أية مســؤوليات شخصية. الآن تــم إزالة هذه العقبة. وأصبح واجباً أن يصدق الرئيس التنفيذي CEO أو المســؤول المالي الأساسي أو غيرهم ممن يمارسون مهام مشابهة على كل تقرير مالي سنوي أو ربع سنوي تم إرســاله. لذلك يجب على المســئول الذي يقوم بالتوقيع، وكجزء مما أشير إليه بالبند ٣٠٢، أن يشهد:

- أن الموظف الذي يقوم بالتوقيع على التقرير قد قام بمراجعته.
- بناء على معرفة هذا الموظف الموقع، فإن القوائم المالية لا تحتوي على أي معلومات مادية مضللة أو غير صحيحة.
- مــرة أخرى فإنه بنــاء على معرفة الموظف الذي يقوم بالتوقيع، فــإن القوائم المالية تُمَثِل بعدالة الأوضاع والنتائج المالية لعمليات التشغيل في المؤسسة.
- أن المسئول الذي يقوم بالتوقيع مسؤول عن:
  - o وضع ضوابط داخلية والحفاظ عليها.
  - o أن تكــون تلــك الضوابط الداخلية قد صُممت لضــمان أن المعلومات الجوهرية عن الشركة والشركات التابعة لها قد تم إعلامها للمسئول الموقع خلال الفترة التي تم فيها إعداد التقارير.
  - o أن تكون الضوابط الداخلية في المؤسسة قد تم تقييمها في غضون ٩٠ يوماً قبل إصدار التقرير.
  - o أن تشــتمل هــذه التقاريــر المالية على تقييــم الموظف الموقع لفاعليــة تلك الضوابط الداخلية حتى تاريخ التقرير.
- يجب أن يفصح المســئول الموقع للمدققين الخارجيــين وللجنة التدقيق ولمديرين آخرين بأنه قد تم الكشــف أو التصريح لمدققي حســابات الشركة عن أي نقص أو خلل مؤثر في تصميم وتشغيل الضوابط الداخلية التي قد تؤثر في دقة البيانات المالية المقدمة.
- ويجب أيضاً على المســئول الموقع أن يشير إلى ما إذا كان هناك ضوابط داخلية أو تغيرات أخرى قد أثرت بشــكل جوهري في تلك الضوابط، وإلى الإجراءات التصحيحية التي جاءت بعد تاريخ تقييم الضوابط الداخلية.

مـن المعلوم أن قانون SOx يفـرض عقوبات جنائية محتملة سـواء بالغرامة المالية أم بالسـجن على الأفراد المخالفين للقانون، كما أن المتطلبات الخاصة بحوكمة المؤسسـة التي قامت بالتوقيع تضع عبئاً ثقيلاً على كاهل المسؤولين في الشركة. لذلك يجب على المسؤولين في الشركة أخذ كل التدابير اللازمة للتأكد من التزامهم بالقانون.

وقد أثار هذا المطلب الخاص بالتوقيع الشـخصي مخاوف كبيرة لدى الرؤسـاء التنفيذيين CEOs والمديرين الماليين CFOs في الشركات كما تسبب في وجود قدر كبير من العمل الإضافي بالنسـبة لموظفي قطاعي المحاسـبة والمالية من أجل تحضير تلك التقارير وكذلك للمسئولين الموقعـين. تحتاج المؤسسـة لوضع إجراءات تفصيليـة لمعالجة البيانات الظاهرة في أسـفل الوثيقـة بحيث يكون المديرون الموقعون مطمئنين إلى اسـتخدام عمليات فعالة وحسـابات لإعداد تقارير جميعها موثقة بشـكل جيد. قد ترغب المؤسسـة في اسـتخدام عملية مطولة للحصول على التوقيعات النهائية، التي يتم اسـتخدامها لكي يقوم الموظفون الذين يُسـلمون التقارير المالية بالتوقيع على ما يقومون بتسليمه. الشكل التوضيحي (٢-٣) يوضح مثال لأحد أنواع الإقرارات الخاصة بموافقة المسـئول على الإفصاح والتي يطلب من المسـؤولين التوقيع عليها. وبالرغم من أن هذا الإقرار الموضح في هذا الشكل ليس أحد النماذج الرسمية الخاصة بمجلس الإشراف المحاسبي على الشركات المساهمة، فإنه يستند إلى وثائق هيئة الأوراق المالية والبورصة الأمريكية، ويوضح أنواع الأمور التي سـيطلب من المدير المسؤول التصديق عليها. لقد قمنا بتسـليط الضوء عـلى عبارتين من العبارات الموجودة في الشـكل التوضيحي (٢-٣) بوضعهما بخط عريض ومائل. وفقاً لقانون SOx فإن الرئيس التنفيذي CEO أو المدير المالي CFO مطالب بالتصديق الشـخصي على هذه الأنواع من البيانات وقد يكون عرضة لمسـاءلة جنائيـة في حالة عدم صحة ما صدق عليه. وعلى الرغم من المخاطرة التي يتعرض لها المدير المسئول، فإنه يجب على فريق الدعم، متضمناً ذلك المدققين الداخليين، أخذ كل الاحتياطات اللازمة والممكنة للتأكد من صحة البيانات المقدمة للمسؤول الأعلى.

الباب الرابع لقانون SOx: تعزيز حالات الإفصاح عن البيانات المالية:

تـم تخصيص هذا الباب من قانون SOx لتصحيح بعض المشـاكل المتعلقة بالإفصاح عن التقارير المالية وللتشـديد على قواعد تضارب المصالح بالنسبة للمسئولين والمديرين،

وإلــزام الإدارة بعمل تقييم للضوابط الداخلية، والمطالبة بعمل مدونة لقواعد الســلوك خاصــة بكبار المديريــن وغيرها من الأمور، حيــث يوجد هنا العديد مــن الأدوات. إن العديــد من حالات الإفــلاس غير المتوقعــة والإخفاقات المفاجئة في جنــي الأرباح التي وقعــت تقريباً في الوقت الذي انهارت فيه شركة إنرون نحو عام ٢٠٠٢ م قد نُسِــبت إلى تقارير مالية شــديدة العدوانية، إن لم تكن محل شــك. فقد لجأت الشركات وبلا حدود وبموافقــة المدققين الخارجيين إلى اتباع بعض الأســاليب غير اللائقــة كالإعلان عن أرباح وهمية غير صحيحة في النتائج المدونة في التقارير، أو القيام بتحويل مقر قيادة الشركة إلى الخارج لتقليص حجم الضرائب. وعلى الرغم من أن هذه الأساليب كان يُسمح بها سابقاً وفقاً للمبادئ المحاســبية المقبولة قبولاً عامــاً GAAP، والمعايير الدولية لإعداد التقارير الماليــة (International Financial Reporting Standards (IFRS) وبعض القوانين الموضوعة وقتها، فإن قانون SOx قد غير هنا العديد من القواعد وجعل من الصعب أو من غير القانوني استخدام مثل هذه الأساليب في الإفصاحات المالية.

إحدى الأساليب التي شاعت وقتها، هو ما كان يطلق عليه تقارير مالية صورية وقد استخدمت هذه الأساليب مراراً وتكراراً لتقديم صورة "وصفية" عن الوضع المالي للشركة مــن خلال إغفال نفقات الأرباح غير المتكررة مثل تكاليــف إعادة الهيكلة أو التكاليف المتعلقــة بالاندماج. من ناحية أخرى، فبســبب عدم وجــود تعريف معياري موحد أو شــكل ثابت للتبليغ عن الأرباح الشــكلية، واعتماداً على الافتراضات المســتخدمة، فقد كان من الممكن أن تصبح خســائر التشــغيل أرباحاً في تقارير الأرباح الصورية. كانت المشــكلة بالنســبة لهاتين المجموعتين من الأرقام أن المســتثمرين والصحافة في معظم الأحيان يتجاهلون أرقام المبادئ المحاســبية المقبولــة قبولاً عاماً GAAP، ويركزون أكثر على النتائج الشــكلية التي يفضلونها. تتطلب القواعد الإلزامية لقانون SOx أنه يجب ألا تحتــوي القوائــم المالية المعلنــة على أي بيانات مادية غير حقيقيــة أو أن تهمل أية حقيقــة يمكن أن تجعــل التقرير مضللاً. إضافــة إلى ذلك، فإن النتائــج الصورية أيضاً يجب أن تتوافق مع الظروف والنتائج المالية لعمليات التشغيل وفقاً للمبادئ المحاسبية المقبولة قبولاً عاماً GAAP.

شكل توضيحي (٢-٣)

إقرار المسئول بالإفصاح طبقاً لقانون SOx

إقرار الموظف بخصوص الامتثال لقانون SOx
هذه ***شــهادة*** إحاطة بأننا نعتزم الاعتماد على هذه البيانات، وإن الموقع أدناه يشــهد، ويقدم ويتعهد لكل منها (هذه البيانات) وللشركة بالتالي: ١. أنني قرأت تلك الأجزاء من المسودة المرفقة بالمغلف والتي تتصل بشكل مباشر بنطاق مسئوليتي كموظف بالشركة ("المعلومات المعتمدة"). ٢. استناداً إلى معرفتي فإن المعلومات المعتمدة وحتى نهاية الفترة التي يغطيها هذا المغلف ***لا تحتوي على بيــان مالي غير صحيــح لأي واقعة مادية*** ولم تهمل الإفصاح عن واقعة مادية ضرورية تجعل البيانات - في ظل الظروف التي أعدت فيها البيانات - غير مضللة. ٣. اســتناداً إلى معرفتي فإنه في حــدود نطاق المعلومات المعتمدة، فــإن المعلومات المعتمدة قد تم تقديمها بصورة نزيهة، في جميع النواحي الجوهرية، والوضع المالي، ونتائج العمليات، والسيولة النقدية للشركة كما في نهاية الفترة المعروضة في المغلف أو على مقربة منها. ٤. لســتُ على علم بأي قصور في فاعلية ضوابط وإجراءات الإفصاح الخاصة بالمؤسسة والتي قد تؤثر بصورة ســلبية في قدرة الشركة في تسجيل، ومعالجة، وتلخيص، وإعداد تقرير عن المعلومات المطلوب الإفصاح عنها في المغلف. ٥. ***لستُ على علم بأي قصور ملموس أو نقطة ضعف جوهرية*** في تصميم وتشغيل الضوابط الداخلية في الشركة والتي قد تؤثر بصورة سلبية على قدرة الشركة في تسجيل، ومعالجة، وتلخيص وإعداد تقارير البيانات المالية. ٦. ***لســت على علم بأي احتيال، ســواء كان مادياً أم غير مادي***، فيما يخص إدارة الشركة أو موظفين آخرين من الذين يلعبون أدواراً أساسية في الضوابط الداخلية للشركة. التوقيع: ______________________ التاريخ: __________ يوم_ _ _ ٢٠xx الاسم: ______________________ المسمى الوظيفي: __________________

ربما كانت القضية الأبرز التي أسهمت في إسقاط شركة إنرون هي وجود عدد كبير من المعاملات الخارجة عن الميزانية العامة التي لو تم دمجها بالتقارير المالية المعتادة، لاتضحت المشاكل المالية الرئيسية. وبمجرد اكتشافها وتضمينها مع النتائج المالية الأخرى لشركة إنرون والإفصاح عنها، قد دفع ذلك شركة إنرون نحو الإفلاس. أما الآن فيشترط قانون SOx إعداد تقارير ربع سنوية وسنوية للإفصاح فيها عن مثل هذه العمليات التي تتم خارج الموازنة والتي قد يكون لها تأثير جوهري في التقارير المالية الحالية أو المستقبلية. قد تتضمن هذه العمليات التزامات طارئة Contingent obligations، أو علاقات مالية مع كيانات غير موحدة، أو أمور أخرى قد يكون لها تأثيرات مادية على عمليات التشغيل. تشترط القواعد النهائية هنا — بعد تمرير قانون SOx — أن تقوم كل مؤسسة بتقديم توضيح عن إجراءاتها المتعلقة بالخروج عن الميزانية "مناقشة وتحليل الإدارة" Management's Discussion and Analysis (MD&A) في النموذج السنوي 10K.

أحكام وإفصاحات وقواعد أخلاقية موسعة لمعالجة تضارب المصالح:

صورت جلسات الاستماع التي أدت إلى إقرار قانون SOx في كثير من الأحيان مسئولي ومديري الشركات بأنهم جشعون وطماعون بشكل كبير. فبعض الإجراءات كانت تبدو متضاربة في المصالح، بدلات الانتقال الضخمة أو القروض الشخصية التي مُنحت للمديرين التنفيذيين في الشركات وتم إعفاؤهم من سدادها بعد ذلك بأمر من مجالس إدارة الشركات، فالرئيس التنفيذي CEO، على سبيل المثال، عندما يطلب من مجلس إدارة الشركة أن يتم منح قرض شخصي لمديره المالي CFO بشروط سداد غامضة مع أحقية المطالبة بسداده أو الإعفاء منه، فإن هذا بالتأكيد يخلق حالة من تضارب المصالح. وعلى الرغم من أن هناك مجموعة من الاستثناءات المسموح بها، فإن قانون SOx اعتبر أنه من غير القانوني بالنسبة لأي شركة أن تقوم، سواء بشكل مباشر أو غير مباشر بتمديد الائتمان - المعطى في صورة قرض شخصي - لأي مسئول أو مدير.

ولكونه أحد العناصر الهامة في الحوكمة المؤسسية، يطالب قانون SOx جميع المؤسسات باعتماد مدونة خاصة بقواعد السلوك المهني وأخلاقيات المهنة لكبار المديرين الماليين لديها

وأن تفصــح عن الالتزام بهــذه المدونة باعتبارها جزءاً من تقاريرهم المالية الســنوية. وفي الوقــت الذي جعل فيه قانون SOx هــذا الأمر أحد المتطلبات الخاصة بكبار المســؤولين، فقد كانت هناك مدونات معتمدة لقواعد السلوك الوظيفي والأخلاقي في بعض المؤسسات لســنوات عديدة. وقد قامت تلك المؤسســات بتطويرها إلى إدارات أكثر رسمية لأخلاقيات المهنة في الشركات الكبرى، وكان ذلك في مطلع التســعينيات من القرن الماضي، إلا أنها كانت توضع غالباً من أجل الموظفين والمشرفين بدلاً من وضعها لمسئولي الشركات. وقد تم في هذه المدونات تعريف مجموعة من القواعد أو السياســات التي تم تصميمها لتطبق على جميع الموظفين، والتي شــملت العديد من المسائل مثل السياسات المفروضة على حماية سجلات الشركة أو السياسات المفروضة على قبول الهدايا وغيرها من القضايا والفوائد الأخرى.

في ظل نمو الاهتمام العام حول الحاجة إلى ممارســات قوية للحوكمة وأخلاقيات العمل، فقد قامت العديد من المؤسسات بتعيين موظف مسؤول عن أخلاقيات المهنة لإطلاق مثل تلــك المبــادرة، من خلال مدونة لقواعد الســلوك في خطوة أولى. ولم يتنــاول قانون SOx محتوى مدونة أخلاقيات المهنة هذه على مســتوى المؤسســة، ولكن ركــز على الحاجة إلى المعايير نفســها بالنسبة لكبار المسؤولين كما هي لجميع الموظفين الآخرين في الشركة. كما يطالب قانون SOx على وجه التحديد أنه يجب على مدونة قواعد السلوك المهني أو مدونة أخلاقيات المهنة الخاصة بكبار مسئولي المؤسسة أن تعزز وبصورة معقولة:

- السلوك النزيه والأخلاقي، متضمناً ذلك التعامل الأخلاقي مع التضارب الفعلي أو الظاهري في المصالح بين العلاقات الشخصية والعلاقات المهنية.
- إفصاح شامل ودقيق وعادل في الوقت المناسب ومفهوم في التقارير المالية للمؤسسة.
- الامتثال للقوانين واللوائح الحكومية المعمول بها.

إذا كانت المؤسسة تمتلك مدونة خاصة بالقواعد السلوكية، فيتعين على الإدارة التأكد من أن هــذه المدونة يتم تطبيقها على جميع أعضاء المؤسســة، وأنها متوافقة مع قانون SOx، وأن هــذه القواعد الأخلاقية قد تم الإفصاح عنها إلى جميع أعضاء المؤسســة، متضمناً ذلك المســؤولين. إن القضية الجوهرية للحوكمة هنــا هي التأكد من أن المدونة الحالية لقواعد السلوك تغطي قواعد قانون SOx السابقة، وأنه قد تم إيصالها إلى الإدارة العليا، وأن هؤلاء

المســؤولين قــد وافقوا على الالتزام بها. وعــلى الرغم من أن عمليات وإجــراءات الامتثال بقانــون SOx قــد وُضعت فقط لكبار المديرين في المؤسســة، فإنه هــذا هو الوقت المثالي لإطــلاق إدارة أخلاقيات المهنة في جميع أنحاء المؤسســة والتي يمكــن تطبيقها على الإدارة العليا وكذلك جميع الموظفين.

ليــس الأمر مطلبــاً شرعياً لقانون SOx فحســب، إذ إن مجموعة فعالــة من المعايير الأخلاقية يمكن أن تعبر بالمؤسسة من وضع كارثي وتساعدها على التحول في الاتجاه الصحيح. كان الدافــع وراء ســن قانون SOx وأحكامه القوية في هذه المجــالات هو إدراك أن بعض مســئولي الشركات كانوا يعملون بهدف تحقيق مصالح ومكاســب شخصية دون أي اعتبار للقيم الأخلاقية الراســخة كما ثبت من خلال التقارير المالية الدقيقة والسليمة. وتستطيع المتطلبات الأخلاقية للمهنة في قانون SOx أن تساعد أي مؤسسة على أن تضع لنفسها قدماً من أجل تحسين الممارسات المتعلقة بالحوكمة وسلوكيات الأعمال الأخلاقية بشكل أفضل.

قواعد ومتطلبات أخرى لقانون SOx:

يتضمن قانون SOX مجموعة كبيرة ومعقدة من القواعد والأحكام التي تغطى مجالات عديدة كالمتطلبــات الخاصة بحوكمة لجنــة التدقيق، وتضارب مصالح المحلل الأمنــي وغيرها من قواعد الإفصــاح المالي. لســنا هنا بصدد تقديم شرح تفصيلي عن كامل القانــون وأحكامه. فمن منظور الحوكمة المؤسســية وحوكمة تقنية المعلومات، فإن فهم وإدراك البند ٤٠٤ وبعض القضايا الأخرى التــي تم تســليط الضوء عليها في هذا الفصل ربما يكون هــو الأكثر أهمية. ويمكن إيجاد الوصف العام الأكثر تفصيلاً لقانون SOx في الكتاب الذي أشار إليه المؤلف سابقاً حول قانون SOx.

يعد قانون SOx منذ إقراره قانوناً أمريكياً في مطلع التســعينيات من القرن الماضي أحد العناصر الهامة في التشريع، فقد أسهم منذ ذلك الوقت في تغيير العديد من القضايا المتعلقة بالتقارير المالية، والممارســات الخاصة بالرقابة الداخلية، والحوكمة المؤسسية. وعلى الرغم مــن بعض التغيرات التي طرأت على بعض عناصر قانــون SOx منذ صدوره وأن متطلباته لا تثــير الكثير من الاهتمام، فإن معظم جوانب قانــون SOx لاتزال فعالة وقابلة للتطبيق. لقد كان الجزء الأكبر في التغيير هو إطلاق معيار التدقيق رقم ٥ AS5، وقد تمت مناقشــته من قبــل، وهو أحد معايير التدقيــق التي تصف نهجاً أكثر اعتماداً عــلى المخاطر لمراجعة

وتقييــم الضوابط الداخلية. وقد احتــوى قانون SOx في الأصل على بعض القواعد الخاصة بالتبليغ عن المخالفات التي سمحت لجميع الموظفين بكتابة تقارير بصورة مستقلة للتبليغ عــن أي احتيال مالي محتمل. وكانت تُصرف مكافآت وحوافز مادية لأصحاب تلك التقارير الشخصية الخاصة بالتبليغ. وعلى الرغم من أنه كان من المفترض أن يتسبب ذلك في عاصفة مــن الدعــاوي القضائية، فإنه لم يكن هناك الكثير منها لأي نشــاط من الأنشــطة الخاصة بقانون SOx في هذا الجانب منذ إقراره وتمريره.

وعــلى الرغم من أنه ســيتم تناول العديد من التفاصيل الخاصــة بهذا القانون من قِبل كل مــن الإدارة المالية والمدققين الداخليين والخارجيين، فإنه يجب أن يكون لدى المســئول التنفيــذي للأعــمال اليوم إدراك عام جيــد لقواعد ومتطلبات قانــون SOx. كما يجب أن يساعد الوصف العام لهذا القانون الذي جاء في ثنايا هذا الفصل مسئولي الأعمال التنفيذيين اليوم على فهم قانون SOx وأهميته في حوكمة تقنية المعلومات على نحو أفضل.

ما المقصود بحوكمة تقنية المعلومات:

كــما هــو موضــح في مقدمة هــذا الفصل، فــإن نظام حوكمــة تقنيــة المعلومات IT Governance عبارة عن مجموعة فرعية من القضايا الشــاملة لحوكمة المؤسســات وأحد العنــاصر الهامــة للغاية في هــذا المجال. لا يوجــد تعريف واحد معتمــد لحوكمة تقنية المعلومات، ويوضح البحث من خلال شــبكة الإنترنــت أن حوكمة تقنية المعلومات تعني أشياء مختلفة لأشخاص مختلفين:

- تُستخدم حوكمة تقنية المعلومات في كثير من الأحيان لوصف العمليات الضرورية لاتخاذ قرار بشأن الأموال التي يجب إنفاقها على موارد تقنية المعلومات. تتضمن عملية حوكمة تقنيــة المعلومــات هذه وضع أولويات للاســتثمارات في تقنية المعلومــات وتبريرها. كما تتضمن الضوابط المفروضة على الإنفاق مثل الموازنات ومستويات الصلاحية.

- تســتخدم حوكمة تقنيــة المعلومات في كثير مــن الأحيان لوصف العديــد من الجوانب المختلفة في التغيرات التي تطرأ على تقنية المعلومات. فعلى المستوى الأدنى، قد تستخدم في بعــض الأحيان لوصف إدارة المشــاريع والتحكم في محفظة المشــاريع المتعلقة بتقنية المعلومات. كما هو موضح في الفصل السادس عشر من هذا الكتاب.

- تستخدم حوكمة تقنية المعلومات لضمان امتثال عمليات التغيير في تقنية المعلومات للمتطلبات التنظيمية سواء كانت قوانين ولوائح حكومية أم معايير مهنية.

- حوكمة تقنية المعلومات هي عملية المواءمة بين التغيير المطلوب في تقنية المعلومات والإنفاق عليها وبين متطلبات الأعمال ونفقاتها. وقد تشمل حوكمة تقنية المعلومات في بعض الأحيان أيضاً آلية توزيع وانتشار فريق تقنية المعلومات.

- تُستخدم حوكمة تقنية المعلومات أيضاً لوصف إدارة وضبط خدمات تقنية المعلومات. على سبيل المثال، تستخدم اتفاقيات مستوى الخدمة service level agreements SLAs (التي سنتحدث عنها في الفصل السابع عشر من هذا الكتاب) لتحديد مستويات الخدمة المقبولة للأعمال، ثم استخدمت بعد ذلك أساساً لمتابعة الخدمات.

- تضمن حوكمة تقنية المعلومات حل المشاكل اليومية وكذلك دعم جميع موارد تقنية المعلومات لتتماشي مع متطلبات العمل.

تتعامل حوكمة تقنية المعلومات بشكل أساسي مع العلاقة بين تركيز أعمال المؤسسة (ما تركز عليه أعمال المؤسسة) وإدارة وتشغيل تقنية المعلومات في المؤسسة. يُبرز مفهوم حوكمة تقنية المعلومات أهمية الأمور المتعلقة بتقنية المعلومات، كما يؤكد ضرورة أن تكون القرارات الإستراتيجية لتقنية المعلومات بيد أعلى مستويات الإدارة في الشركة متضمناً مجلس الإدارة بدلاً من أن تكون بيد إدارة تقنية المعلومات فقط مثل الرئيس التنفيذي للمعلومات CIO. في الواقع، لقد تطورت مفاهيم حوكمة تقنية المعلومات منذ الأيام الأولى لظهور تقنية المعلومات عندما تخلت الإدارة العليا في كثير من الأحيان عن سلطة عمليات تشغيل تقنية المعلومات وتمويلها لصالح أخصائيين يُطلق عليهم الرؤساء التنفيذيون للمعلومات CIOs، ولكنهم لم يديروا موارد تقنية المعلومات بقوة من منظور الإدارة الشاملة.

وقد كانت نتائج تلك العملية في الواقع متمثلة في ظهور بعض العمليات الممتازة لتقنية المعلومات التي أحدثت تحولاً كبيراً في العديد من الشركات الرائدة في جميع أنحاء العالم وحسنت من كفاءاتها وزادت من أرباحها، ومع كل ذلك، فقد عانت العديد من المؤسسات الأخرى من بعض الإخفاقات الجسيمة (الانهيار الكلي) في تقنية المعلومات،

وكان ذلك بسبب التخطيط السيئ للمشروعات، تجاوز التكاليف، وإخفاقات على مستوى فهـم القائمين على الأعمال وتقنية المعلومات لقضايا تقنية المعلومات، وغيرها من الأمور. على سـبيل المثال، كشف استطلاع رأي أجرته مؤسسـة غارتنر في عام ٢٠٠٢ أن ٢٠٪ من مجموع الأموال التي تـم إنفاقها على تقنية المعلومات قد أُهدرت، وهذه النتيجة تمثل، عـلى الصعيد العالمـي، تدميراً لما قيمته الإجمالية قرابة ٦٠٠ مليار دولار أمريكي سـنوياً. وقد كشـف الاسـتطلاع الذي أجرته شركة آي بي إم (IBM) سـنة ٢٠٠٤ لأكبر ١٠٠٠ من الرؤسـاء التنفيذيين للمعلومات CIOs بأنهم يعتقدون أن، في المتوسـط، قرابة ٤٠٪ من مجمل الإنفاق على تقنية المعلومات لم يحقق أي عوائد لمؤسسـاتهم[٤]. وفي السـنوات الأخيرة، كشفت استطلاعات رأي أخرى أن ما بين ٢٠٪ إلى ٧٠٪ من الاستثمارات الضخمة في مشـاريع تقنية المعلومات يتم إهدارها بصفة مسـتمرة، مما يعد عائقاً أو إخفاقاً في تحقيق أي عوائد أو فوائد لمؤسساتهم. كل ذلك يشير إلى الحاجة إلى نظم قوية لحوكمة تقنيـة المعلومات المؤسسـية. فبدلاً مـن الجدل القائم حول تحديـد التعريف الأفضل والأصلـح لحوكمة تقنيـة المعلومات، فإنه يجب على كبار مديري المؤسسـات النظر إلى عناصر التشابه بين جميع التعريفات الواردة. ففي كل حالة تقريباً تشتمل الحوكمة على مزيجٍ مما يلي:

- التحكم في جميع الجوانب الخاصة بعمل تقنية المعلومات.
- التنسـيق بين الأجزاء المختلفة للأعمال المرتبطة بتقنيـة المعلومات — مثل تطوير النظم الجديدة للبنية التحتية لتقنية المعلومات.
- قياس مخرجات نظم وعمليات تقنية المعلومات.
- الامتثال للسياسات الداخلية لتقنية المعلومات.
- تبرير الإنفاق على جميع موارد تقنية المعلومات.
- المساءلة والشفافية على مستوى إدارة تقنية المعلومات والمؤسسة.
- روابط قوية مع الاحتياجات الخاصة بعملاء تقنية المعلومات، وواسعة النطاق للمؤسسة، وغيرهم من أصحاب المصلحة.

إن العديد من قضايا حوكمة تقنية المعلومات تلك معنية بسمات نظم تقنية المعلومات نفسها متضمنة قضايا التقنية الحديثة، والنظم القديمة التي تستخدم تقنيات قديمة، الأمن والتوثيق، والعديد من القضايا الأخرى. إن معالجة مثل تلك المسائل الخاصة بحوكمة تقنية المعلومات ليست بالأساس مسألة تقنية، وإنما هي مسألة إدارية.

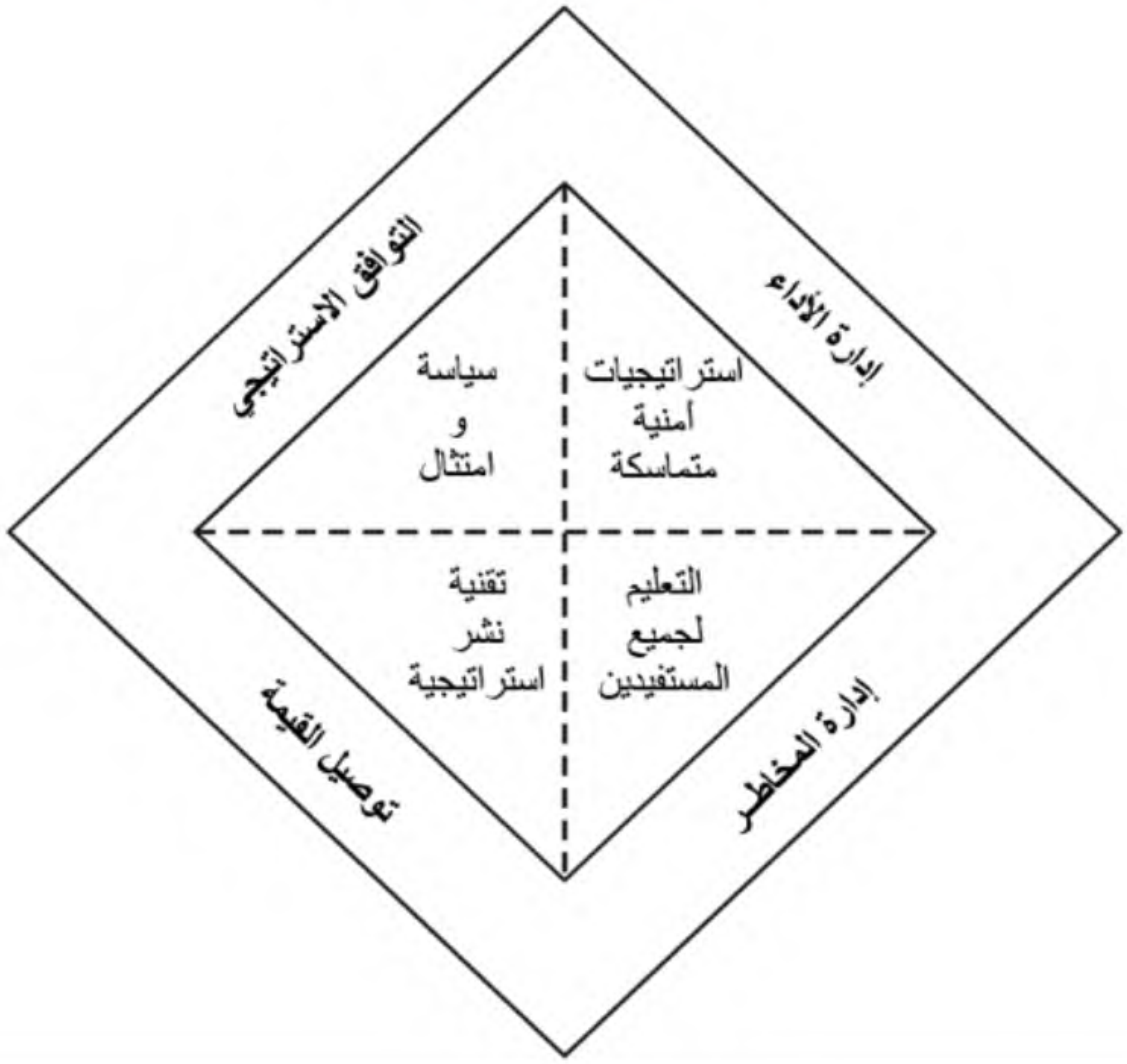
لعل السمة الأبرز في القضايا الخاصة بحوكمة تقنية المعلومات في هذا الفصل وغيره من الفصول اللاحقة هي أن موارد وقدرات تقنية المعلومات في المؤسسة لم تعد شيئاً غير مفهوم من جانب الأعمال في المؤسسة، على الجانب الآخر يتعين أيضاً على تقنية المعلومات هذه أن تفهم الأعمال واحتياجاتها. يجب أن تكون القضايا الجوهرية لتقنية المعلومات إحدى المسائل التي تخص المديرين التنفيذيين على مستوى مجلس الإدارة، إلا أنه بسبب الطبيعة التقنية لتقنية المعلومات قد تُترك بعض القرارات الرئيسية لأخصائيي تقنية المعلومات. إن حوكمة تقنية المعلومات عبارة عن النظام الذي يملك فيه جميع أصحاب المصالح، ومن ضمنهم مجلس الإدارة والعملاء المحليون وغيرهم كالمالية، المدخلات الضرورية لعملية صنع القرار.

ستناقش الفصول التالية العديد من الجوانب والافتراضات المتعلقة بحوكمة تقنية المعلومات. وستركز بشكل عام على قضايا المخاطر المؤسسية، وقضايا حوكمة تقنية المعلومات، ومسائل قانونية ونظامية وقضايا أمن المعلومات، والتهديدات الداخلية والخارجية التي تؤثر في حوكمة تقنية المعلومات.

تتوافق جميع أهداف حوكمة تقنية المعلومات داخل نموذج شامل، كما هو موضح بالشكل التوضيحي (٢-٤). تكون حوكمة تقنية المعلومات محاطة بمفاهيم إدارة الأداء، والتوافق الإستراتيجي، وإدارة المخاطر، وتوصيل القيمة. ولتحقيق ذلك، هناك حاجة إلى سياسة قوية، وممارسات امتثال، وعمليات لإدارة الأداء والمخاطر، وفهم شامل للتوصيل المناسب للقيمة. يعرض الشكل التوضيحي (٢-٤) هذه المفاهيم على مستوى رفيع، غير أنه سيتم الرجوع إليها بالتفصيل في فصول لاحقة.

شكل توضيحي (٢-٤)

أهداف حوكمة تقنية المعلومات



قضايا المخاطر المؤسسية لحوكمة تقنية المعلومات:

تواجه كل مؤسسة مجموعة كبيرة من المخاطر، تشمل عمليات تشغيل الأعمال المؤسسية، والعوامل الخاصة بسوق العمل وما يتصل بها، والأوضاع الاقتصادية العامة، وقائمة غير منتهية من العوامل الأخرى من المخاطر المؤسسية. وعلى الرغم من أن هذا الكتاب لا يسعى لتقديم ومناقشة جميع الجوانب الرئيسية المتعلقة بإدارة المخاطر على مستوى المؤسسة وما يعرف بإطار عمل إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية [٥] (COSO) enterprise risk managemen (COSO ERM)؛ فإن هناك العديد من الجوانب المتعلقة بالإدارة الشاملة للمخاطر المؤسسية، وهي جوانب هامة بالنسبة

للممارســات الفعالة لتقنية المعلومات على وجة التحديد. ســيقدم الفصل الرابع من هذا الكتاب معلومات أكثر حول لجنة المنظمات الراعية COSO.

ولكي تمتلك المؤسســة ممارســات فعالة لحوكمة تقنية المعلومــات، فهي بحاجة إلى أن يكون لديها برنامج فعال لتقييم وإدارة المخاطر الشــاملة، والمخاطر المؤثرة داخل المؤسسة، والمخاطر النوعية التي تواجة عمليات التشــغيل الخاصة بتقنية المعلومات. يعرض الشكل التوضيحــي (٢-٥) بإيجاز بعض القضايــا الخاصة بمخاطر حوكمة تقنية المعلومات ويلخص بعض الإستراتيجيات الفعالة في إدارة تلك المخاطر.

ما يواجه كبار المديرين غالباً اعتراضات شديدة أو بسيطة عندما يقومون بقبول وإدارة العديــد من أنواع المخاطــر المتعلقة بتقنيــة المعلومات. خير مثال عــلى ذلك كلمة السر المســتخدمة في النظم للوصول لموارد تقنية المعلومــات. فتبعاً لأحد الاتجاهات، قد يحتاج المدير غير الملم بالتقنية بشــكل جيد إلى أن يســتخدم أسلوباً بســيطاً وسهلاً التذكر لكلمة المرور، والتي تكون غالباً مكونة من ثلاثة حروف تمثل الأحرف الأولى من اسمه الثلاثي ورقم. فالســيدة Mary Anne Jones قد تستخدم MAJ1 كلمة مرور للوصول إلى النظم الخاصة بهــا، ويمكن تغيير كلمة المــرور فقط من خلال تغيير الرقم المكــون من عدد واحد من آن لآخر عند تغيير كلمات المرور. وبذلك يكون هذا النظام ســهل التذكر ولكن يمكن اختراقه بسهولة.

يؤيــد أخصائيو أمن المعلومات عادة الذهاب إلى الاتجاه الآخر وهو وضع معايير لكلمة المــرور، تكون غالباً مركبــة من ثمانية حروف أو أكثر منها حــروف كبيرة وصغيرة، بالإضافة إلى الأرقــام والرموز الخاصة وجميعها تتطلب تغييراً بصفة دورية. قد يخلق ذلك جواً أكثر أماناً وسرية، إلا أن الكثيرين قد تكون لديهم مشــكلة في استدعاء كلمات المرور هذه والتي يصعب تذكرها، ومن ثم يقومون بكتابتها على أوراق ملاحظات لاصقة ووضعها على لوحات المفاتيح الخاصة بحواسيبهم.

شكل توضيحي (٢-٥)

قضايا مخاطر حوكمة تقنية المعلومات

متطلبات المخاطر المؤسسية	استراتيجيات تفعيل المخاطر
فهم رغبة المؤسسة في المخاطر	عندما تُوَاجَه المؤسسة بمخاطر اختيارية. فعليها أن تدرك مدى حجم ومستوى المخاطر التي ستتحملها. فعندما تكون الإدارة مستعدة لقبول مشاريع أكثر مخاطرة، ينظر إليها بأن لديها شهية كبيرة للمخاطر.
فهم قبول المخاطر	ستواجه المؤسسة مخاطر عديدة. ولكن يجب أن يكون هناك فهم كافٍ وواضح لتحديد أي وحدة داخل المؤسسة هي التي ستقبل المخاطرة أو تتحمل مسئوليتها.
ضمان مشاركة الأشخاص المناسبين	يجب إسناد مسؤوليات الوحدة التنظيمية عن جميع المخاطر المحددة. كما يجب على الوحدة التنظيمية الإقرار بمسؤوليتها عن اتخاذ الإجراءات المناسبة في حال وقوع المخاطر.
قبول المخاطر المتبقية	من وجهة نظر المحاسبة أو التدقيق، تعتبر المخاطر المتبقية هي احتمالية أن المدقق لن يستطع الوصول إلى الخطأ الجوهري الموجود في التقرير المالي للعميل ومن ثم سيقدم بشكل خاطئ تقريراً لا يحمل أي تحفظات حول دقّة الحسابات. وبالمفهوم نفسه، قد تكون الإدارة غير مدركة للآثار المترتبة على المخاطر ومن ثم تقبل المخاطر أو تقر بهذه الأشياء.
فهم عمليات اختيار الرقابة	تحتاج المؤسسة إلى معرفة تكاليف ومقتضيات الضوابط المختلفة التي يمكن أن تقوم بوضعها استجابة لمختلف المخاطر المحددة.
معرفة تكاليف معالجة أحداث المخاطر	ستواجه المؤسسة العديد من المخاطر، لذا يجب أن يكون لديها معرفة جيدة بالتكاليف اللازمة لمعالجة مختلف الأمور في حال وقوع المخاطر المحددة.

وضع إستراتيجية واضحة للتخفيف من المخاطر	يجب أن يكون لدى المؤسسة إستراتيجية محددة ومسببة على نحو جيد حول ماهية الإجراءات أو التدابير التي يجب اتباعها في حال حدوث مخاطر مرتبطة بتقنية المعلومات.
فهم عمليات اختيار الرقابة	هنـاك العديد من الاعتبارات في حـال حدوث مخاطر مرتبطة بتقنيـة المعلومات. لذا يجب على المؤسسـة أن تقوم بتطوير الضوابـط الملائمـة التي سـوف تقـوم بمعالجة تلـك المخاطر بطريقة فعالة.

إن الفكرة الرئيسية وراء متطلبات وإستراتيجيات المخاطر الموضحة في الشكل التوضيحي (٢-٥) هو أن المؤسسـة بحاجة إلى أن يكون لديها معرفـة بمختلف أنواع المخاطر المتعلقة بتقنية المعلومات التي تواجهها وكذلك التكاليف والإسـتراتيجيات البديلة لاتخاذ الإجراءات التصحيحيـة المتبعة في حال وقـوع مثل تلك المخاطر. إن المصطلـح أو المفهوم الهام جداً هنا هو ما يسـمى الرغبة في المخاطر Risk Appetite. بمعنى، ما حجم المخاطر التي على اسـتعداد أن يتقبلها أحد كبار المديرين أو المؤسسة بأكملها؟ فالمستثمر الفردي الذي يضع أمواله في سـندات شركة تصنيفها (AA) يمتلك شـهية مخاطر أقل بكثير من المستثمر الذي يضع أمواله في سوق أسهم شركات التقنية المضاربة.

إن الإلمـام بقضايا المخاطر المؤسسـية يعد مطلبـاً لتطبيق العمليـات الفعالة لحوكمة تقنيـة المعلومات. إننا في الواقع نحتـاج دائماً إلى أن ندرك أن كل مجال من مجالات تقنية المعلومات وعمليات التشغيل الشاملة للأعمال تشتمل على مخاطر لأنشطة أو أحداث غير مخطط لها. لذلك يجب أن يكون لدينا دائماً إستراتيجيات وعمليات معمول بها للاستجابة بشكل ملائم لتلك المخاطر في حال حدوث أي منها.

قضايا التنظيم المؤسسي لحوكمة تقنية المعلومات:

لقد توسـعت قضايا واهتمامات حوكمة تقنية المعلومات لتصل إلى ما هو أبعد من إدارة تقنيـة المعلومات ومواردها فقط، بل يجب أن تشـمل العديد من القضايا والاهتمامات على مسـتوى المؤسسـة بأكملها. لذلك يجـب علينا أن ننظر دائماً إلى مـورد تقنية المعلومات في

المؤسســة بأنه ليس مجــرد عنصر متفرد بل هو أحد الوحــدات أو المكونات التي لها طبيعة خاصة بالنســبة للمؤسســة بأكملها. بعض تلك القضايا الخاصة بالحوكمة موضحة بالشــكل التوضيحي (٢-٦).

إن الرســالة التي يريد الشــكل التوضيحي (٢-٦) أن يبعث بهــا هي أنه على الرغم مــن أن إدارة تقنيــة المعلومات قد تقوم بتطوير عمليات وإجــراءات للحوكمة تؤثر في نظم وعمليات تشــغيل تقنية المعلومــات الخاصة بها فإنه يجب عليهــم التفكير دائماً في تلــك العمليــات والإجراءات في إطار أكبر من ذلك بكثير يشــمل المؤسســة بأكملها. فعلى ســبيل المثال، من الســهل جداً نســيان أن هناك العديد من الإجــراءات الخاصة بالحوكمة تؤثر في المســؤولية الائتمانية للمؤسســة وفي مديريها الأساسيين بوجه خاص للحفاظ على استثمارات المستثمرين وتعزيزها على جميع المستويات. إذ يمكن أن يؤدي الإخفاق أو القصور في هذا الأمر إلى رفع الدعاوى المدنية أو حتى القانونية على مديري المؤسســة. والاعتبار الذي له صلة هنا هو أن المؤسســة وعملياتها التشــغيلية الخاصة بتقنية المعلومات لا يملكون مجموعة مفتوحة أو غير منتهية من الموارد لأخذ الإجراءات التصحيحية المناسبة. لذا يجب أن نوازن دائماً بين أثر اتخاذ الإجراءات التصحيحية وبين موارد المؤسسة بأكملها.

يشــير الشــكل التوضيحي (٢-٦) إلى قضايا الاختصاص والحدود على أنها أحد مكونات حوكمة تقنية المعلومات. فمع أنه قبل سنوات ليست بالكثيرة كانت موارد تقنية المعلومات في المؤسسة توضع خلف أبواب مغلقة محكمة السرية وتكون غالباً مرفقة في موقع منعزل عن باقي العمليات التشغيلية للمؤسسة، إلا أن هذا لا يجب أن يمنعنا في أن ننظر دائماً إلى العمليات التشــغيلية الخاصة بتقنية المعلومات على أنها العنصر الرئيسي في عملية استمرار باقي العمليات التشغيلية الأخرى في المؤسسة. على أية حال، يجب علينا أن نتذكر دائماً أن هناك حدوداً موجودة، ويجب أن تدرك العمليات التشغيلية التقنية والمالية وغيرها الحدود بين مختلف مجالات المسؤولية عند وضع عمليات الحوكمة.

حوكمة تقنية المعلومات والقضايا التشريعية والتنظيمية:

بدأنا هذا الفصل بتقديم نبذة مختصرة عن بعض العناصر الأساسية في قانون SOx، وهو أحد العناصر الهامة في التشريع التي تؤثر في المراجعة والتقارير المالية وضوابطها الداخلية. وبالرغم من احتوائه على العديد من القواعد التشريعية الرئيسية، فإن SOx هو مجرد قانون من بين العديد من القوانين التنظيمية والتشريعية الرئيسية وحتى القوانين الثانوية التي تؤثر في العمليات التشغيلية لحوكمة تقنية المعلومات. يغطي بعض هذه القوانين كامل العمليات التشغيلية المؤسسية على المستوى المحلي أو الدولي. في حين يختص البعض الآخر بشكل أكبر بأمن تقنية المعلومات. وفي حالات أخرى، نجد أن العمليات التشغيلية لحوكمة تقنية المعلومات لا تتأثر بالقواعد والقوانين التشريعية الحكومية، ولكنها تتأثر بالمعايير المهنية غير الإلزامية ولكنها ضرورية للبقاء على الأقل في المنافسة.

ستقدم الفصول اللاحقة وتناقش بعض القضايا التشريعية والتنظيمية المتعلقة بحوكمة تقنية المعلومات بمزيد من التفصيل. على سبيل المثال، يقدم الفصل العاشر من هذا الكتاب نبذة عامة عن بعض من بين العديد من قوانين أمن تقنية المعلومات التي تؤثر في المؤسسة هذه الأيام. ويناقش الفصل الحادي عشر العناصر الهامة الخاصة بمعيار أمن البيانات الخاص بصناعة بطاقات الدفع Payment Card Industry Data Security Standard (PCI DSS)، التي تعتبر مجموعة هامة من القواعد المؤثرة في أي مؤسسة تستخدم بطاقات الائتمان في العمليات التشغيلية الخاصة بأعمالها. وعلى المستوى الآخر، يقدم الفصل السابع من هذا الكتاب بعض المعايير العالمية في حوكمة تقنية المعلومات مثل معيار أيزو٣٨٥٠٠ (ISO 38500)، والتي لا تعتبر قواعد تشريعية بل معايير امتثال يجب اتباعها من قبل أي مؤسسة ذكية.

شكل توضيحي (٢-٦)

قضايا حوكمة تقنية المعلومات المؤسسية

القضية على مستوى المؤسسة	الاعتبارات الخاصة بحوكمة تقنية المعلومات
عمليات رصد المخاطر في الشركات	هـي أكثر مـن مجرد تحديد لأنواع ومسـتويات مختلفـة للمخاطر المؤسسـية والتقنية التي يمكـن أن تؤثر في المؤسسـة، لذا يجب أن تكون هناك عمليات معمول بها ومستمرة لتحديد حالة تلك المخاطر المحددة إلى جانب وجود خطط عمل سارية وذلك لاتخاذ الإجراءات المناسبة في حال وقوع المخاطر.
الآليات الضعيفة لاتخاذ القرارت	هـي أكثر من مجـرد مراقبة لحالة المخاطر المتعلقـة بحوكمة تقنية المعلومـات، لذا يجـب أن تكون هناك عمليـات إدارية معمول بها لاتخاذ الإجراءات المناسبة في حال وقوع المخاطر. ويعتبر ذلك صعباً خاصة في حال اشـتمل الإجراء المخطط له على بعض الأمور كإيقاف تشغيل الشبكة التقنية، وهو الأمر الذي يتطلب قرارات إدارية قوية وحاسمة.
مخاطر انتهاك خصوصية سجلات البيانات الخاصة وبيانات الأعمال	سـواء كانت سجلات أعمال أم سجلات مالية أو بيانات شخصية، فإن المؤسسة تحتفظ في سـجلاتها وأنظمتها بكميات هائلة من البيانات والمعلومات التي يجب حمايتها.
مخاطر الإلزام غير الفعال وفض النزاعات	تطبـق قضايا حوكمة تقنية المعلومـات غالباً على أنماط محدودة أو متعـددة من الإجـراءات التصحيحية ذات الأهميـة التي تتخذ عند تنفيذ الإجراءات المناسـبة. لذا يجب أن تكون هناك عمليات إدارية نظامية وقوية ومجربة.
مخاطر شح الموارد المالية	في حـين أنه من السـهل في بعض الأحيـان بالنسـبة للمختصين أن يقوموا بتطوير خطة علاجية للمخاطر، إلا أن قلة الموارد المالية لدى المؤسسة قد تحول دون استخدام تلك الخطة.

مخاطر الإخفاق في فهم جميع مسؤوليات الأعمال وحاجات أصحاب المصالح	تركز إدارات تقنية المعلومات غالباً على العمليات التشغيلية الخاصة بالبنية التحتية لتقنية المعلومات الخاصة بها ولكنها تخفق في فهم متطلبات ومخاطر العملية الشاملة للمؤسسة، وكذلك تلك التي تخص أصحاب المصالح كالباعة والموردين الرئيسيين.
مخاطر المسؤوليات الائتمانية	على جميع المستويات، تحتاج المؤسسة وعمليات تشغيل تقنية المعلومات(الخاصة بها أو التابعة لها) أن يتذكروا دائماً أن لديهم واجب حماية الأصول والاستثمارات الخاصة بأصحاب المصالح والمقرضين.
مخاطر تحديد الحدود والسلطة	في كثير من الأحيان، نرى أن أنشطة مراقبة ومعالجة المخاطر تمتد لتتجاوز عمليات تشغيل تقنية المعلومات لتصل إلى المؤسسة بأكملها وإلى جميع أصحاب المصالح الآخرين الرئيسيين. لذا فهناك حاجة ماسة للتعرف على السلطات والحدود

تعتبر القواعد والقضايا التنظيمية والتشريعية من العناصر الهامة في العمليات الفعالة لحوكمة تقنية المعلومات. فعلى إدارة المؤسسة مراقبة تلك القواعد واتخاذ الخطوات المناسبة للتأكيد على الامتثال بها.

شكل توضيحي (٢-٧)

قضايا الأمن الخاصة بحوكمة تقنية المعلومات

قضايا أمن تقنية المعلومات	أنشطة حوكمة تقنية المعلومات
مخاطر السياسات والإجراءات الأمنية	يجب أن يكون لدى المؤسسة إجراءات قوية لكشف ومنع محاولات الاختراقات والتطفلات الخاصة بأمن تقنية المعلومات. ويجب أن يكون هناك أيضاً فريق مختص ومهاري لمراقبة أمن تقنية المعلومات واتخاذ الإجراءات التصحيحية إذا تطلب الأمر.
قضايا التخطيط لاستمرارية الأعمال	يجب أن يكون هناك عمليات مفعلة لاسترجاع العمليات التشغيلية في حال حدوث اضطرابات غير متوقعة للعمليات التشغيلية والنظم. ويجب فحص هذه النظم بالكامل للمحافظة على الوضع الراهن لتعكس التغيرات الحاصلة في العمليات التشغيلية المؤسسية.

مخاطر البرمجيات الضارة	يجــب أن تدرك الإدارة أن جميع الأنظمة هــذه الأيام عرضة لمجموعة واسعة ومتطورة باستمرار من البرمجيات الضارة التي لديها المقدرة على تخطي عمليات الكشف عنها بحيث تقوم بتغيير نفسها بمجرد إطلاقها.
متطلبات الكشف الفعال للتسلل وأدوات مراقبة أمن تقنية المعلومات	يجــب أن تعمل المؤسســة على إيجاد الأدوات اللازمــة لمراقبة جميع الجوانــب المتعلقة بأمــن تقنية المعلومات، عــلى الصعيدين الداخلي والخارجي، واتخاذ الإجراءات العلاجية الفعالة عند الحاجة.
مخاطر تصنيف أصول تقنية المعلومات	يجــب تحديد جميع أصول تقنية المعلومات من البرمجيات والمعدات بشكل مناســب، وتحديد نقاط الضعف الأمني الخاصة بها مع خطط أعمال تصحيحية مجربة ومطبقة ومفعلة.
مخاطر مراقبة أمن تقنية المعلومات	يجب أن تكون هناك أدوات معمول بها لرصد ومراقبة جميع الجوانب المتعلقــة بأمن تقنية المعلومات والبدء بالإجراءات الملائمة عند تحديد أي اختراقات أو هجمات أمنية.
مخاطر سياسات التشفير وإدارته	يجب إيجاد سياســات تشفير فعالة واستخدامها عند الضرورة لتحسين الممارسات الخاصة بحوكمة تقنية المعلومات.
مخاطر أمن تقنية المعلومات الخاصة بأصحاب المصلحة	يجب توافر سياســات وأدوات تدريبية لضمان اتبــاع جميع أصحاب المصلحة المعنيين في المؤسسة لإجراءات مناسبة لأمن تقنية المعلومات.

القضايا الأمنية لحوكمة تقنية المعلومات:

نظراً لترابط العمليات التشغيلية لتقنية المعلومات في المؤسسة على الصعيدين الداخلي والخارجــي من خــلال الإنترنت والعديد مــن الروابط الأخرى، فإن أمــن تقنية المعلومات يعتــبر من القضايا الرئيســية في حوكمة تقنية المعلومات. حيث يــدرك العديد من عملاء ومســتخدمي تقنية المعلومات أن نظمهــم وبياناتهم عرضة لشريحة واســعة من الدخلاء والمتطفلــين من الذين تتراوح اهتماماتهم من مجرد التشــويش على العمليات التشــغيلية لتقنية المعلومات لصالح جهة ما إلى أن تصل إلى حد تخريب النظم والبيانات لتحقيق بعض المكاســب. لذا يعتبر وجود الضوابط الفعالــة لأمن تقنية المعلومات من العناصر الهامة في حوكمة تقنية المعلومات.

يحــب أن يكون لــدى المدير التنفيذي هــذه الأيام معرفة عامة عالية المســتوى في القضايــا الأكثر تأثيراً في أمن تقنية المعلومات والمهمة بالنســبة للحوكمة الفعالة لتقنية المعلومــات. فمــع أن هناك العديد مــن القضايا المختلفة في هذا المجــال، فإنه يجب على مديــر الأعمال أن يفهم التهديدات والمخاطر الخاصــة بتقنية المعلومات بل يجب عليه أيضاً البحث عن مســاعدة تقنية متخصصة بداخل المؤسسة لتقوم بتطبيق الأنواع الموضحة بالشكل التوضيحي (٢-٧) للعمليات الأمنية الخاصة بحوكمة تقنية المعلومات بشكل أكثر فاعلية.

التهديدات الداخلية والخارجية لحوكمة تقنية المعلومات:

بالإضافــة لقضايــا حوكمة تقنية المعلومــات الأكثر تخصصية، فإن المؤسســة تتعرض لحجم هائل من التهديدات الأمنية الداخلية والخارجية. فقد تمتد التهديدات الخارجية من مجرد أمور أشبه بالهجوم الإرهابي الذي تقوم به إحدى الحكومات الأجنبية المتورطة بقضايا التجســس إلى أن يصل إلى مخاطر تتعلق بالحوسبة السحابية وأكثر. فعلى الرغم من أننا ســوف نناقش بعض التهديدات التقنية المتعلقة بالحوســبة السحابية في الفصل التاسع من هذا الكتاب، فإن المؤسسة تواجه هذه الأيام مجموعة واسعة من التهديدات الخارجيــة التي تهدد مواردها التقنية والعمليات التشــغيلية الخاصة بأعمالها أيضاً. لذا يتعــين على المدير التنفيذي في هــذه الأيام التأكد من أنه تم الاســتعانة بأدوات مراقبة ورصد مناسبة وبأشخاص مهرة لمراقبة مثل تلك التهديدات واتخاذ الإجراءات التصحيحة المناسبة.

يمكن مراقبة عمليات حوكمة تقنية المعلومات الخاصة بالتهديدات الداخلية والتحكم بها بشكل أفضل في أغلب الأحيان. ومع أننا لا نعرف مطلقاً الوقت الذي سيقوم به بعض الدخلاء غير المتوقعين بمهاجمة نظم تقنية المعلومات الخاصة بنا، فإننا نســتطيع تقليص مخاطــر التهديدات الداخلية عن طريق وضع سياســات وإجراءات داخلية قوية تشــمل العديــد من تلك السياســات والإجراءات التي تمت مناقشــتها في هــذا الفصل إلى جانب بناء فريق مؤســسي يدرك فيه جميع أصحاب المصالح لأدوارهم ومسؤولياتهم ولتوقعات الإدارة.

كما ذكرنا في هذا الفصل، فإن حوكمة تقنية المعلومات هي المجال الواسـع الذي يشمل العديد من المجالات الخاصة بالعمليات التشـغيلية المؤسسـية وتتجة جيداً إلى ما هو أكثر من مجرد إدارة تقنية المعلومات. وهي أكثر بكثير من الموضوع السـاخن الحالي الذي يثير ضجة كبيرة. لذا يجب أن يعمل كبار المديرين التنفيذيين في المؤسسـة اليوم جنباً إلى جنب مـع الكادر التقني وأخصائيي أمـن المعلومات لديهم إلى جانب المدققين الداخليين لتطوير ممارسـات قوية لحوكمة تقنية المعلومات. سـتقدم الفصول اللاحقة المزيد من المعلومات والنقاشات التي تدور حول تطبيق ممارسات فعالة في حوكمة تقنية معلومات.

ملاحظات:

1. عـلى الرغـم من أننا نقـدم مجرد ملخص عالي المسـتوى لمتطلبات قانـون SOx ، فإن Robert Moeller, Sarbanes-Oxley Internal Controls: Effective Auditing" "(with AS5, CobiT, and ITIL (Hoboken, NJ: John Wiley & Sons, 2008 يقدم الكثير والمزيد من المعلومات.

2. عـلى اعتبار أنها وثيقة عامة، فإنه يمكن العثور عـلى نص القانون في العديد من مواقع الويب. أحد هذه المصادر هي:

http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/gwbush/.sarbanesoxley072302.pdf

3. كأحـد مبادئ القانون: حتى لو ظهر انتهاك اصطلاحي للقانون طبقاً لنص القانون، فإن كان تأثيره صغيراً جداً بحيث لا يكون له أي عواقب، فإن انتهاك القانون في هذه الحالة لن يعتد به كسبب كافٍ لاتخاذ أي إجراء، سواء كانت هذه الإجراءات مدنية أم جنائية.

4. Steve Crutchley, “IT Governance Helping Business Survival,” www.slideshare.net/khanyasmin/it-governance-consult2comply.

5. لمزيد من المعلومات حول إدارة المخاطر المؤسسية و إدارة المخاطر المؤسسية الخاصة بلجنة المنظـمات الراعية (COSO ERM) انظـر " Robert Moeller's COSO Enterprise "(Risk Management, 2nd ed. (Hoboken, NJ: John Wiley & Sons, 2011."

الفصل الثالث

حوكمة المؤسسات وأدوات الحوكمة وإدارة المخاطر والامتثال GRC

واجهت جميع الشركات التجارية والشركات المساهمة العامة بصفة خاصة منذ نشأتها قضايا تتعلق باحتياجات ومتطلبات الحوكمة. فبالنسبة للعديد من المؤسسات، كانت الإدارة العليا غالباً هي التي تأخذ زمام المبادرة في البداية للقيام بوضع سياسات وقواعد الامتثال للأعمال التي يجب التقيد بها واتباعها من قبل موظفيها وغيرهم. وبالرغم من أن ذلك كان مناسباً بالنسبة للملكيات الفردية الصغيرة أو للشركات المركزية التي كانت موجودة في العصور الماضية، فإن العديد من المؤسسات الكبيرة المتعددة الوحدات تحتاج إلى تسهيلات على نطاق واسع لوضع مثل هذه السياسات والإجراءات، أي أنها بحاجة إلى عمليات حوكمة ذات كفاءة وفاعلية.

ستكون الحياة أسهل بكثير بالنسبة لبعض المؤسسات التي تعتمد فقط على قيادة مركزية قوية، رئيس تنفيذي CEO مهيمن، ليفوض ويدير مباشرة تطبيق أي قاعدة من القواعد المطلوبة للحوكمة. من ناحية أخرى، تُوَاجَه الشركات في هذه الأيام على مختلف أماكنها وأحجامها بمجموعات متزايدة وبشكل غير مسبوق من القواعد والإجراءات التي تمتد من السياسة المحلية وقوانين السلامة العامة إلى القوانين واللوائح الحكومية التي تصدر على مستوى الولاية والمستوى الوطني، وفي بعض الأحيان على المستوى الدولي، هذا بالإضافة إلى وجود مجموعة كبيرة من القواعد المهنية الهامة. ويتعين على المؤسسة أن تلتزم بتلك اللوائح والقوانين والقواعد على جميع المستويات. وقد يترتب على عدم التزام الشركة بها فرض العديد من العقوبات الجزائية عليها. فكل مؤسسة تحتاج إلى عمليات تضمن التزامها بالقوانين والتشريعات الضرورية.

تكون المؤسسة دائماً عرضة للمخاطر التي تتعلق بعدم فهم أو تفسير القواعد كما ينبغي أو قيامها بانتهاك واحد أو أكثر من القوانين والنظم التشريعية المتعددة. كما يوجد

هنــاك مخاطر أيضاً تتعلق بعدم قــدرة قواعد الحوكمة التي قامت المؤسســة بوضعها على تحقيق النتائج المرجوة، أو أن تواجه المؤسســة بعض الأحداث الخارجية الطارئة الخارجة عن سيطرتها، كحدوث تحولات اقتصادية كبيرة، أو التعرض لهجمات إرهابية أو تحولات اقتصادية كبيرة تؤثر في منطقة عملياتها التشغيلية، أو اندلاع حريق في أحد المرافق الرئيسية للمؤسسة. لذا فهناك حاجة إلى فهم وإدارة جميع تلك المخاطر على مستوى المؤسسة بأكملها.

وعــلى الرغم من أن المؤسســة تكون دائماً قلقة إزاء العديد مــن القضايا المختلفة التي تخــص الحوكمة، وإدارة المخاطر، والامتثال. إلا أن الســمة الرئيســية لهذا الكتاب أنه قام بجمع كل من هذه المخاوف الثلاثة معاً في سياق تقنية المعلومات وفيما يعرف أيضاً بمبادئ الحوكمــة وإدارة المخاطر والامتثال جي آر سي (GRC). وبينما ســتناقش الفصول القادمة قضايا أهمية ممارســات الحوكمة المؤسسية وأساســيات إدارة المخاطر وممارسات حوكمة الشركات، سيركز هذا الفصل على أهمية إنشاء مجموعة قوية من مبادئ الحوكمة المؤسسية وإدارة المخاطــر والامتثــال أو ما يعرف بمبــادئ GRC، التي تعد أحــد العناصر الهامة في حوكمة تقنية المعلومات.

الطريق نحو مبادئ فعالة للحوكمة وإدارة المخاطر والامتثال GRC:

حتــى مطلع القــرن الحالي لم يكن أحد من المهنيين قد ســمع بمصطلح GRC الشــائع بكثرة هذه الأيام. حيث يشــير الحرف الأول في هذا المصطلح إلى الحوكمة Governance، ليســت حوكمة تقنية المعلومات فحسب، إنما هي حوكمة الأمور المتعلقة بكامل المؤسسة. باختصار، فإن الحوكمة تعنــي الاهتمام بالأعمال ورعايتها والتأكد من أن جميع الأمور تتم وفقاً للمعايير واللوائح التنظيمية للمؤسسة وكذلك قرارات مجلس إدارة المؤسسة، بالإضافة إلى القوانين والقواعد الحكومية. وهي تعني أيضاً طرح توقعات أصحاب المصلحة بشــكل واضح فيما ينبغي عمله كي يكون أصحاب المصالح جميعهم متفقين على الهدف نفسه فيما يخص الكيفية التي تعمل بها المؤسسة.

في حين يشــير الحرف R في المصطلح GRC إلى المخاطر Risk. فكل ما نقوم به وكذلك الجوانب المتعلقة بعمليات تشــغيل الأعمال قد ينطوي على نوع ما من المخاطرة. فعندما يتعلــق الأمر مثلاً بأحد الأشــخاص الذي يجري عبر أحد الطرق السريعــة، أو الطفل الذي

يلعب بأعواد الثقاب، فمن الواضح هنا أن هذه المخاطر المؤكدة لا يجب قبولها بالمرة. أما عندما يتعلق الأمر بالأعمال، فإنه ومع ذلك تصبح عوامل المخاطرة طريقة للمساعدة في حماية قيم الأصول الحالية، هذا من جانب، ومن جانب آخر طريقة لخلق قيم جديدة من خلال التوسع الإستراتيجي للشركة أو إضافة منتجات وخدمات جديدة.

وأخيراً يشير الحرف الأخير C في هذا المصطلح GRC إلى الامتثال، أي التقيد أو الالتزام بالعديد من القوانين والتعليمات التي تؤثر في الأعمال والمواطنين اليوم. وأحياناً يقوم الناس بتوسيع مفهوم الامتثال ليشمل أيضاً الضوابط الرقابية Controls، وهذا يعني أنه من المهم وضع ضوابط محددة موضع التنفيذ للتأكد من تحقيق الامتثال. على سبيل المثال، قد نقصد بذلك القيام بمراقبة الانبعاثات الخاصة بأحد المصانع أو التأكد من أن المستندات الخاصة بوارداته وصادراته سليمة ومطابقة للنظام. أو أنها قد تعني فقط وضع ضوابط جيدة للمحاسبة الداخلية وتطبيق متطلبات تشريعية بطريقة فعالة مثل القواعد الخاصة بقانون SOx التي سبق مناقشتها باختصار في الفصل الثاني من هذا الكتاب. وبضم هذه الحروف جميعها معاً، لا تكون الحوكمة وإدارة المخاطر والامتثال GRC هو ما يجب أن تفعله لرعاية المؤسسة فحسب، إنما هو عبارة عن نموذج أولي يساعد في نمو تلك المؤسسة بأفضل وسيلة ممكنة.

كما ذكرنا في الفقرات التمهيدية، لم يتم مسبقاً التطرق إلى مبادئ الحوكمة وإدارة المخاطر والامتثال GRC والنظر إليهم على أنها مجموعة موحدة من المبادئ من قبل جميع المؤسسات، والشركات على وجه الخصوص. فبمقدار ما كانت المؤسسة تدير أو تهتم بأي من هذه المجالات الثلاثة، بقدر ما كانت غالباً تديرهم معاً بصورة أقل كفاءة عما إذا تمت إداراتهم كمجالات أو اهتمامات منفصلة. إن إدارة المخاطر هنا هي الحالة التقليدية، فقد فكرت المؤسسات بإدارة المخاطر من ناحية التغطية التأمينية، وقامت بإدارة مخاطرها من خلال إدارة التأمين إذ إنها كانت في أغلب الأحيان لا تملك الكثير لتفعله حيال العمليات التشغيلية الأخرى في المؤسسة. وكذلك بالنسبة للامتثال، فنحن بحاجة دائماً للتوافق مع جميع مستويات الإجراءات الموضوعة، متضمناً ذلك القواعد التي تم وضعها للمساعدة في إدارة المؤسسة. ولكن لم يسبق على مر التاريخ أن قمنا بدمج هذه المجالات الثلاثة معاً لتشكل ما يعرف

بمبادئ الحوكمة وإدارة المخاطر والامتثال GRC. فمصطلح GRC اليوم متعارف عليه بشكل متزايد حيث يعكس أسـلوباً جديداً تستطيع المؤسسات من خلاله اعتماد نهج متكامل لدمج تلك الجوانب الخاصة بأعمالهم، كما أنه يعكس أسلوباً جديداً يُمَكن المؤسسات من اعتماد نهج موحد ومتكامل لجميع الجوانب الثلاثة في قالب واحد أثناء إتمام أعمالهم.

بالذهـاب إلى أبعد مـن كونه مجرد اختصار، نجـد أنه من المهم تذكـر تلك المجالات المحورية لكل من الحوكمة وإدارة المخاطر والامتثال. فكل مجال من هذه المجالات يتكون من أربعة مكونات أساسية لنموذج GRC وهم: الإستراتيجية، والعمليات، والتقنية، والناس.

يوضح الشكل التوضيحي (٣-١) هذه المفاهيم الخاصة بمبادئ GRC، فمبادئ الحوكمة وإدارة المخاطـر والامتثال يجب أن تكون محاطة بإحكام لربط هذه المبادئ معاً. ويوضح الشكل أيضاً أن السياسات الداخلية هي العوامل الرئيسية التي تدعم الحوكمة، وأن اللوائح التنظيميـة الخارجيـة هي التـي تقود مبادئ وقواعـد الامتثال، وأن ما نُطلـق عليه رغبة المؤسسة في المخاطر يعد أحد العناصر الرئيسية في إدارة المخاطر.

يعتـبر مصطلح الرغبة في المخاطـر Risk appetite من المصطلحـات الجديدة نوعاً ما بالنسبة للعديد من المهنيين في مجال الأعمال وتقنية المعلومات. فهو يشير إلى مقدار ونوع المخاطر التي تستطيع المنظمة متابعتها وتحملها. فعلى سبيل المثال، المستثمر الذي يضارب بأمواله فيما يطلق عليه غالباً بـ "الأسـهم ذات الدولار الواحد Penny Stocks" التي تكون محفوفة بالمخاطر، تكون لديه رغبة عالية في المخاطر، في حين أن المسـتثمر الذي يسـتثمر أمواله في صناديق سـوق المال الآمنة تكون لديه رغبة منخفضة في المخاطر. ويمكن تطبيق السيناريو نفسه على العديد من قرارات الاعمال المؤسسية.

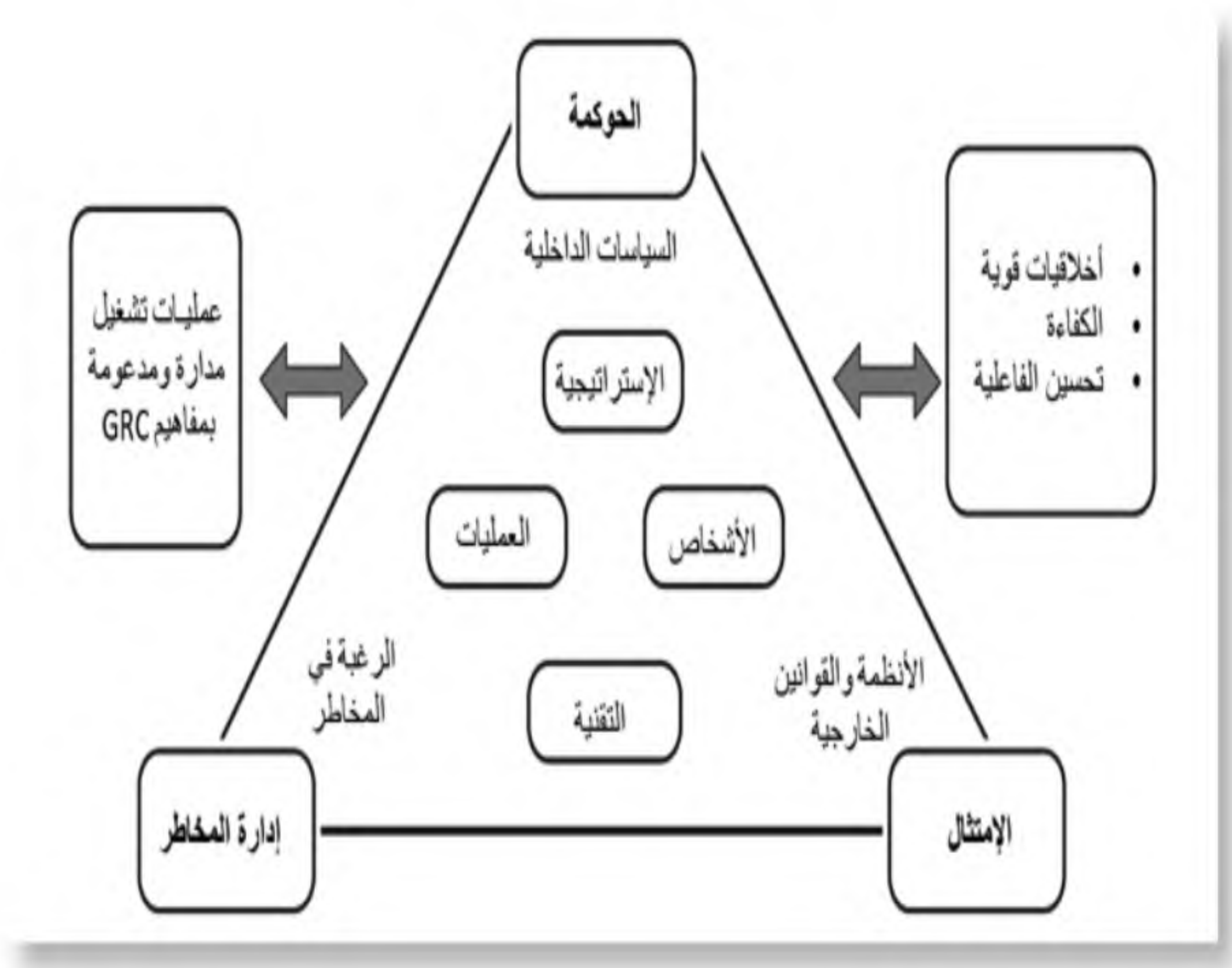
يوضح الشكل التوضيحي (٣-١) أيضاً مكونات الإستراتيجية، والعمليات الفعالة، والتقنيات (بما فيها تقنية المعلومات IT)، والناس داخل المؤسسة للقيام بكل هذا العمل. وعلى الجانب الأيسر للمثلث من الخارج، يوضح الشكل حاجة المؤسسة لاهتمام ودعم الإدارة وأن السلوك الأخلاقي السليم والكفاءة التنظيمية وتحسين الفاعلية تعد من العناصر الأساسية. وستتناول الأقسـام التالية من هذا الفصل كل مكون من المكونـات الخاصة بنموذج GRC بمزيد من التفصيل، وسنقوم أيضاً بالحديث عن العديد منها في فصول أخرى من هذا الكتاب.

أهمية الحوكمة في نموذج GRC

يجب التفكير بالمبادئ الثلاثة الرئيســية الخاصة بنموذج GRC والداعمة لحوكمة تقنية المعلومات على أنها تيار واحد من المفاهيم المســتمرة والمترابطة بحيث لا يكون لأي منها، سواء الحوكمة G أو إدارة المخاطر R أو الامتثال C، أهمية زائدة عن الآخرين. وحيث إن غالبية الفصــول القادمة تغطي العديد من جوانب حوكمة تقنية المعلومات، فإننا ســنبدأ الحديث هنا عن الجانب الخاص بالحوكمة G في نموذج GRC.

شكل توضيحي (٣-١)

المفاهيم الخاصة بنموذج GRC



حوكمة الشركات أو المؤسسات هو مصطلح يشير بشكل واسع إلى القواعد أو العمليات أو القوانين التي بها يتم تشغيل الأعمال وتنظيمها ومراقبتها. ويمكن أن يشير هذا المصطلح إلى العوامل الداخلية التي تم تحديدها أو تعريفها بواسطة المسؤولين أو أصحاب المصالح أو دستور الشركة، بالإضافة إلى القوى الخارجية كمجموعات المستهلكين والعملاء واللوائح التنظيمية الحكومية.

نزولاً من المستويات العليا للشركة ووصولاً إلى العديد من المجالات الخاصة بالعمليات التشغيلية في الشركة، يمكننا تعريف حوكمة المؤسسات على أنها المسئوليات والممارسات التي يتم تنفيذها من قبل مجلس الإدارة، والإدارة التنفيذية العليا، وجميع المستويات الخاصة بالإدارة الوظيفية العليا، بهدف توفير توجه إستراتيجي، والتأكد من أن الأهداف الموضوعة قد تم تحقيقها، والتأكد من أن المخاطر قد تمت إدارتها بالأسلوب المناسب، وفحص ما إذا كانت موارد المؤسسة قد تم استخدامها بشكل معقول. فالحوكمة في الواقع تشير إلى عملية وضع القواعد والإجراءات في جميع مستويات المؤسسة، وتوصيل هذه القواعد إلى المستويات المناسبة من أصحاب المصلحة، ومراقبة الأداء وفقاً لتلك القواعد، ومن ثم إدارة المكافآت والعقوبات بناء على الأداء أو الامتثال النسبي لتلك القواعد.

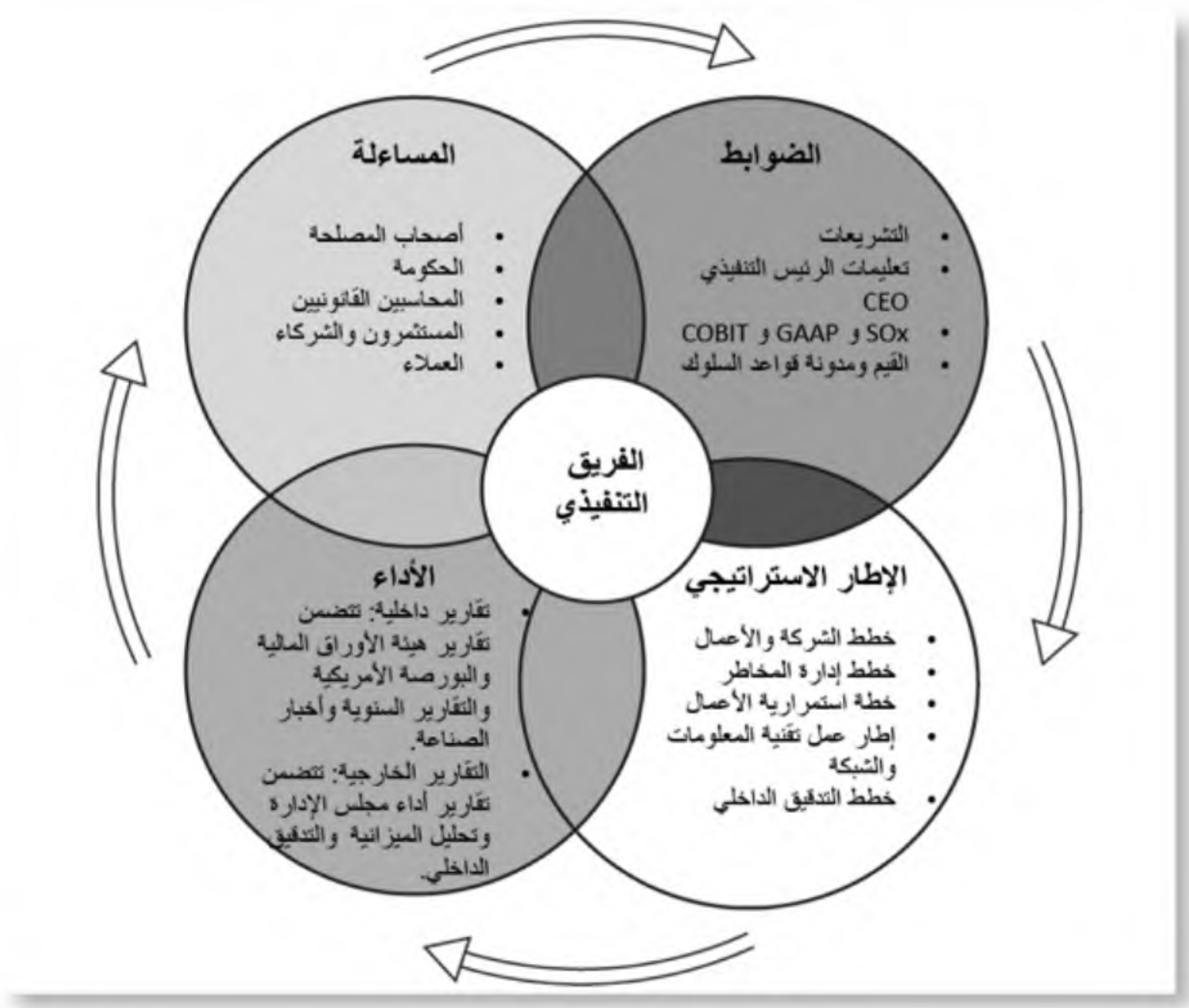
توفر مجموعة مبادئ حوكمة الشركات أو المؤسسات المعرفة بشكل جيد والتي يتم إنفاذها بأسلوب جيد، على الأقل من الناحية النظرية، الأعمال التي تصب في مصلحة كل فرد مهتم بضمان أن تلتزم المؤسسة بالمعايير الأخلاقية المعتمدة واتباع أفضل الممارسات، بالإضافة إلى اللوائح والقوانين والمعايير الرسمية المناسبة. لقد لاقت قضايا حوكمة الشركات المزيد من الاهتمام في السنوات الأخيرة نتيجة الفضائح المدوية الناجمة عن سوء استخدام السلطة في الشركات، وسوء التقديرات المالية، وفي بعض الحالات، ممارسة أنشطة جنائية من قبل مسئولي الشركة. إن وضع أحكام قضائية، سواء كانت مدنية أم جنائية، لإدانة الأفراد الذين يقومون بأعمال لا أخلاقية وغير قانونية باسم الشركة يعد جزءاً مكملاً ومتمماً للنظام الجيد والفعال الخاص بحوكمة الشركات.

وعلى الرغم من أننا كثيراً ما نقوم بوصف جميع مفاهيم الحوكمة الخاصة بالمؤسسات أو الشركات باستخدام القليل من الفقرات القصيرة أو باستخدام صور واحدة، فإن الشكل التوضيحي (٣-٢) يعرض مجالات تتعلق بمفاهيم الحوكمة المؤسسية باستخدام مجموعة تنفيذية في وسط الشكل، كما يوضح الشكل بعض التداخل أو التشارك الموجود بين هذه المفاهيم والمسؤوليات المرتبطة بها من أجل تأسيس كل من الضوابط والإطار الإستراتيجي للأعمال وتحسين الأداء وفرض المساءلة أو المحاسبة. كما يعرض الشكل التوضيحي (٣-٢) أيضاً بعض المفاهيم الرئيسية التي تندرج تحت كل مجال من مجالات المسؤولية تلك. فمثلاً بالنسبة للإطار الإستراتيجي للأعمال، يوجد بها عدة عناصر أو مفاهيم مهمة كأنشطة التخطيط والأعمال المؤسسية وإدارة المخاطر واستمرارية الأعمال وتقنية المعلومات والشبكات والتدقيق الداخلي.

تم تضمين الحوكمة، وهي جزء رئيسي في نموذج مبادئ GRC، في العديد من الفصول اللاحقة والتي تتحدث عن قضايا معينة في حوكمة تقنية المعلومات، ونخص بالذكر هنا كلاً من الفصل الثامن الذي يتحدث عن إدارة المخاطر، والفصل الثامن عشر الذي تناول الحديث عن حوكمة تقنية المعلومات. ويركز الفصل الثامن عشر أيضاً على مسائل متعلقة بتقنية المعلومات وإستراتيجيات الأعمال وعمليات الحوكمة.

شكل توضيحي (٣-٢)

عناصر حوكمة GRC



عنصر إدارة المخاطر في نموذج GRC:

إن الهدف الرئيسي لهذا الكتاب هو تقديم مفاهيم حوكمة تقنية المعلومات إلى مسئولي الأعمال التنفيذيين. فمن الضروري أن يكون هناك مجموعة قوية من مكونات ومبادئ الحوكمة وإدارة المخاطر والامتثال GRC على مستوى المؤسسة بكاملها، ويعد البرنامج الفعال لإدارة المخاطر أحد العناصر الرئيسية لمبادئ GRC في المؤسسة. وسيتم الحديث

بمزيد من التفصيل عن أساسيات إدارة المخاطر وأمن تقنية المعلومات في كل من الفصل الثامن والعاشر من هذا الكتاب، حيث يجب أن تصبح إدارة المخاطر جزءاً من الثقافة العامة للمؤسسة ابتداء من مجلس الإدارة وكبار المسؤولين نزولاً إلى جميع أنحاء المؤسسة. هناك أربع خطوات مترابطة في العمليات الفعالة لإدارة المخاطر المؤسسية وفقاً لنموذج GRC كما هو واضح في الشكل التوضيحي (٣-٣) وهي:

١- **تقييم المخاطر والتخطيط لها:** قد تتعرض المؤسسات إلى مستويات متعددة من المخاطر، سواء كانت قضايا عالمية تتراوح بين أزمات الاقتصاد المحلي أم أزمات العملة، إلى عوامل المنافسة في سوق المنتجات وحدوث اضطرابات في العمليات التشغيلية المحلية نتيجة سوء الأحوال الجوية. وهنا لا يمكننا تعريف كل نوع من أنواع المخاطر التي قد تؤثر في المؤسسة والتخطيط لها، إلا أنه ينبغي أن يكون هناك تحليل مستمر لمختلف المخاطر المحتملة التي قد تواجه المؤسسة.

٢- **تحديد وتحليل المخاطر:** بدلاً من التخطيط فقط لاحتمالية وقوع بعض المخاطر، هناك حاجة ماسة إلى المزيد من التحاليل التفصيلية التي تمكننا من معرفة احتمالية وقوع هذه المخاطر القادمة ومعرفة مدى تأثيراتها المحتملة أيضاً. كما أن هناك حاجة أيضاً لقياس الآثار المترتبة على تلك المخاطر المحددة، وذلك لتحديد إستراتيجيات للعمل على التخفيف من آثارها في حال وقوع أحداث تلك المخاطر. يشير التخفيف هنا إلى تقدير أفضل وسيلة لإدارة المخاطرة أو استبعادها. كما يجب أيضاً تحديد العوامل النهائية المرتبطة بتلك المخاطر. وستصبح المخاطر المحددة أكثر أهمية إذا استطعنا تحديد التكاليف الإجمالية التي ستتحملها الشركة إذا وقعت تلك المخاطر المحددة.

٣- **توظيف وتطوير إستراتيجيات الاستجابة للمخاطر:** يجب أن تضع المؤسسة خططاً وإستراتيجيات واضحة لاستعادة العمليات التشغيلية الطبيعية الخاصة بها والتعافي من أحداث المخاطر التي يمكن أن تحدث، ويجب أن يتم ذلك بشكل أساسي بالتوازي مع تحديد تلك المخاطر. وقد يشتمل ذلك على تحليل الفرص المتعلقة بالمخاطر. فعلى سبيل المثال، إذا كان لدينا أحد المخاطر المحددة سلفاً تخص

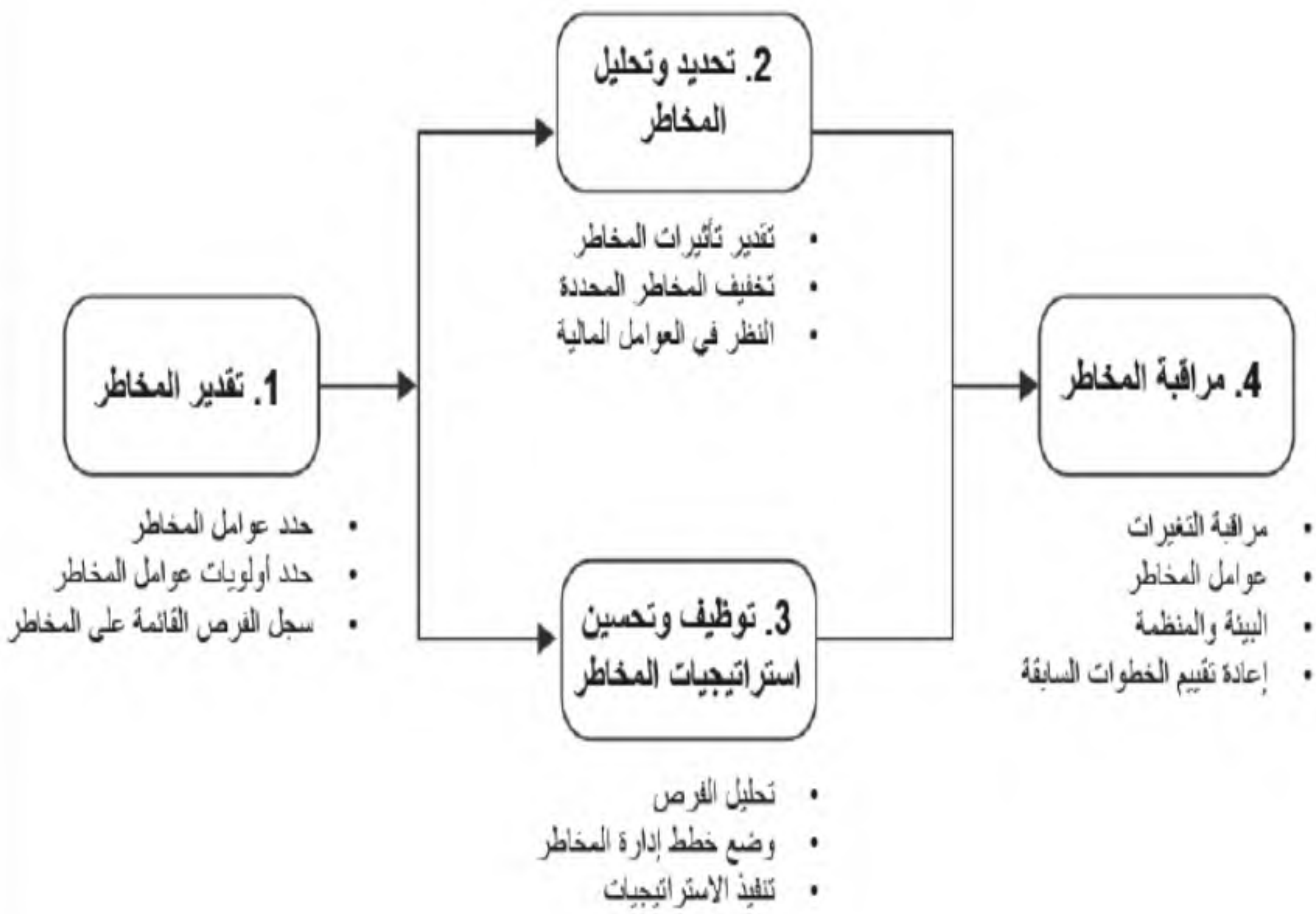
معــدات إنتاج قديمة في أحد المصانــع والتي ربما تتوقف عــن الإنتاج، فقد تكون هذه فرصة للتخلي عن خط الإنتاج هذا وتركيب معدات جديدة تستخدم تقنيات حديثة، أو حتى من الممكن أن تكون فرصة لنقل المصنع إلى موقع أحدث أو موقع بديل للموقع الحالي.

٤- **متابعــة المخاطر:** يجب أن تكون هناك أدوات وتجهيزات معمول بها لرصد جميع المخاطــر المحددة والجديدة أيضاً والتي من الممكن حدوثها، مثل وضع جهاز إنذار حريق للكشف عن الدخان. وبالرغم من أن معظم عمليات مراقبة المخاطر تحتاج إلى سلســلة ممتدة من التقارير الخاصة، وإلى معايير معمــول بها وقابلة للقياس، وإلى إدارة مــوارد بشريــة يقظه، فــإن الفكرة هنا هي أن تكون ســباقاً أو متقدماً بخطوة وتعاود الدخول في تلك الخطوات الســابق ذكرها لإدارة المخاطر إذا اقتضى الأمر ذلك.

يجــب أن تعمــل إدارة المخاطر عــلى إيجاد قيمــة وأن تكون جزءاً متمــماً للعمليات التنظيمية. كما يجب أن تكون جزءاً من عمليات صنع القرار وأن تكون مصممة بأســلوب منهجي ومنظم لمعالجة الشــكوك أو الأحداث المبهمة التي يمكن أن تواجه المؤسسة، وذلك بالاعتــماد على أفضــل المعلومات المتاحة. هذا بالإضافة إلى أنه يجــب أيضاً أن تكون تلك العمليــات الخاصة بإدارة المخاطر مرنة وتكرارية ومســتجيبة للتغيرات من خلال القدرات الخاصة بالتطويرات والتحسينات المستمرة.

شكل توضيحى (٣-٣)

نظرة عامة على إدارة المخاطر



نموذج GRC وامتثال المؤسسة:

الامتثال هو عملية الالتزام أو التقيد بالإرشادات أو بالقواعد الموضوعة من قبل الهيئات الحكوميـة، أو المجموعات المختلفة لوضع المعايير، أو السياسـات الداخلية للشركة. ويعد الالتزام أو التقيد بمتطلبات الامتثال أحد التحديات بالنسـبة للمؤسسـة وأصحاب المصالح لديها، وذلك للأسباب التالية:

- **طـرح لوائح تنظيمية جديدة بصـورة متكررة:** بالنظر إلى الولايـات المتحدة الأمريكية هناك العديد من الوكالات، كوكالة حماية البيئة مثلاً، والتي تقوم وبشكل منتظم بإصدار قواعد جديدة يمكن أن تؤثر بشـكل كبير في العديد من المؤسسات رغم اختلاف أغراضها

الأساسـية. فالتحدي بالنسـبة للشركات هنا هو متابعة تلك القواعد الجديدة لمعرفة أي من هذه القواعد يمكن أن ينطبق عليها.

- **وجود قوانين غامضة وبحاجة إلى تفسير:** وبالنظر مرة أخرى إلى الولايات المتحدة الأمريكية على سـبيل المثال، فقـد أقر الكونجرس الأمريكي مشروع قانون إصـلاح الرعاية الصحية في عام ٢٠١٠، والمعروف باسـم أوباما كير (Obamacare)، والذي تمت صياغته من قبل هيئة مـن أعضاء الكونجرس وطباعته في عدة آلاف مـن الصفحات التي تغطي قضايا وقواعد لم تتـم قراءتها قـط، حتى من قبل المشرعين لهذا القانون، ناهيـك عن إمكانية فهمها. حتى هذه الأيام ولسـنوات قادمة سنظل ننظر إلى هذه القواعد ونحاول تفسير المعاني الحقيقية المقصودة منها. ويمكننا أيضاً الحديث عن قانون دود فرانك Dodd-Frank للإصلاح المالي سـنة ٢٠١١ كمثال آخر مشـابه للمثال السـابق. فهو عبارة عن قانون معقد جداً لتنظيم المجال المالي، ويحتوي هذا القانون على العديد من القواعد الإدارية التي لم تكن قد نشرت بعد حتى وقت إعداد هذا الكتاب. وقد يكون امتثال المؤسسـة لتلك القواعد أمراً في غاية الصعوبة.

- **لا يوجد إجماع على أفضل الممارسـات في الامتثال:** إن القواعد مليئة باللوائح القانونية التي تنص على أمور مثل: "جميع المعاملات التي تتم لابد أن تكون مدعومة بالإيصالات". فهل يشترط هذا القانون استخدام إيصالات في المعاملات التي تقل قيمتها عن ١$ أو عن ٢٥$ أو عن أي قيمة أخرى؟ فلا يوجد هناك أي إرشادات خاصة لتلك القاعدة ويستطيع كل شخص أن يفسرها كما يحلو له.

- **كـثرة تداخل اللوائـح التنظيمية مع بعضها البعـض:** فغالباً ما تقـوم الولايات المتحدة الأمريكيـة والحكومات المحليـة الموجودة في مختلـف الولايات بإصـدار قوانين تغطي المجـالات نفسـها، إلا أن لها متطلبات مختلفة. ويتم البـت في هذه الاختلافات عادة في النهاية داخل سـاحات المحاكم. وتبقي قضية الامتثال أحد التحديات إلى أن يتم الفصل في هذه الأمور.

- **تغير اللوائح التنظيمية بصفة مسـتمرة:** فغالباً ما تقوم الهيئات التنظيمية وبشـكل مسـتمر ودوري بتغيير قوانينها أو التفسيرات المتعلقة بقوانينها، الأمر الذي يجعل الامتثال تحدياً كبيراً.

لا بد من النظر إلى قضية امتثال المؤسسة على أنها عملية مستمرة وليست مشروعاً ينفذ لمرة واحدة فقط. فضلاً عن أن متطلبات الامتثال مستمرة في صدارة جداول الأعمال الخاصة بالمؤسسات، نظراً لأنه يجري محاسبة المؤسسات على وفائها بالتفويضات الكثيرة المتعلقة بأسواقها الخاصة أو مجالات عملياتها التشغيلية.

هذا بالإضافة إلى أن المؤسسات قد تكون مطالبة أيضاً بمعالجة التشريعات التي تتم عبر الأنشطة الصناعية، كمعيار أمن بيانات بطاقات الدفع Payment Card Industry Data Security Standard (PCI DSS) وغيرها من القواعد التي سنتحدث عنها في الفصل الحادي عشر من هذا الكتاب، بالإضافة إلى القضايا الأخرى الخاصة بحوكمة وإدارة تقنية المعلومات التي تم طرحها في الفصل الخامس عشر من هذا الكتاب. ببساطة يمكن القول بأن اتساع دائرة وتعقيد القوانين واللوائح المتعلقة بالامتثال قد تتسبب في وجود تحديات للعديد من المؤسسات على مر السنين. تحتاج المؤسسات إلى الإقبال على مبادئ الامتثال الخاصة بنموذج GRC من منظور أكثر إستراتيجية، الأمر الذي قد يساعدها على الانتقال إلى ما هو أبعد من مجرد الوفاء والالتزام بالقوانين والمعايير والمبادئ المفروضة بل إلى تحقيق فوائد تجارية ملموسة وحقيقية من مجمل استثماراتها في البنية التحتية.

يتخلل نطاق الامتثال العديد من الأنشطة وعمليات التشغيل داخل المؤسسة. ويوضح الشكل التوضيحي (٣-٤) بعض المسائل التي يجب على المؤسسة أن تأخذها بعين الاعتبار عند قيامها بتحديد النطاق والنهج الذي ستستخدمه من أجل تحقيق مبادئ الامتثال الخاصة بنموذج GRC. لذا يجب على المؤسسة ألا تهمل أياً من هذه القواعد وأن تكون دائماً على علم بوجودها. غير أن اتباع نهج منتظم ومتناغم لاستخدام الإمكانيات والتقنيات الداعمة التي تقودها مبادئ الامتثال في جميع أنحاء المؤسسة يمكن أن يسهم في منح المؤسسة العديد من الفوائد المحتملة التالية:

- **المرونة:** تعد الأنظمة التشريعية الجديدة الصادرة عن الهيئات المصرح لها بإصدارها، والتغيير المستمر للقوانين الحالية، واحدة من الصعوبات المتعلقة بعملية الامتثال. فمن خلال إدارة مبادرات الامتثال بشكل مركزي عبر بنية الامتثال على مستوى المؤسسة، يمكن للمؤسسة أن تتكيف وبسرعة أكبر مع هذه التغييرات.

- **انخفاض التكلفة الإجمالية لحيازة الامتثال:** قد يكون هناك تأثير إيجابي في الاســتثمارات جراء العديد من الأنظمة التشريعية. فعلى ســبيل المثال، الاستثمار في نظام إدارة قواعد البيانات والســجلات كان نتيجة مطالبة العديد مــن اللوائح التنظيمية التشريعية للقيام بالاحتفاظ بالوثائق والســجلات الرسمية. الأمر الذي قد يقابل باستثمار فردي في إحدى الوسائل الخاصة بقاعدة بيانات المحتوى ونظام إدارة السجلات.

- **الميزة التنافســية:** قد تسمح بنية الامتثال الواســعة والمتناغمة للمؤسسة بأن تكون أكثر إدراكاً وتحكــماً بعملياتها، الأمر الذي قد يمكنها من سرعة ودقة الاســتجابة والتكيف مع ضغوطــات الامتثال الداخلية أو الخارجية. هذا بالإضافــة إلى احتمالية أن تحتوي بعض الأنظمة التشريعية على العديد من الفوائد التجارية الهامة والملموســة، وذلك من خلال متطلبات كتخفيض الحد الأدنى من رأس المال والتي يمكن تفعيلها من خلال بنية الامتثال على مستوى المؤسسة بأكملها.

تســاعد العمليات الفعالة للامتثــال الخاصة بنموذج GRC المؤسســة أن تقوم بتغيير عمليــات تشــغيل الأعمال لديهــا والحصول على تبــصر وإمكانية توقــع أعمق من خلال المعلومــات التي تخــص الأعمال عندما تقوم بمعالجة المتطلبــات المدفوعة تنظيمياً. ولعل أهم العوامل المحركة للأعمال هنا هي القدرة على تحســين إدارة أصول المعلومات وإثبات الامتثال للالتزامات التنظيمية والقانونية والحد من مخاطر الدعاوى القضائية ومن تكاليف التخزين والاكتشاف وإثبات مساءلة الشركات.

شكل توضيحي (٣-٤)

اعتبارات المؤسسة الخاصة بنطاق أنشطة الامتثال الخاصة بها

النطاق الخاص بمجال الامتثال	دائرة الاهتمام
الاستراتيجية	• يجب أن تحدد المؤسسة اللوائح التنظيمية الأكثر ارتباطاً بأعمالها أثناء تطوير خطتها الإستراتيجية.
	• استدامة الامتثال يجب أن يكون جزءاً أساسياً ومتمماً في أي خطة إستراتيجية للامتثال.
المنظمة	• يجب وضع الهيكل التنظيمي لتلبية متطلبات (او مقاصد) محددة لكل تشريع من التشريعات (فعلى سبيل المثال، يوصي قانون SOx بألا يكون رئيس مجلس الإدارة هو نفسه الرئيس التنفيذي)
العمليات	• يجب توثيق وممارسة العمليات الرئيسية للامتثال.
	• يجب أن تتم عمليات التدقيق والمراجعة للتأكد من أن العمليات الموثقة يتم استخدامها بشكل فعال لمعالجة متطلبات الامتثال.
التطبيقات والبيانات	• التطبيقات يجب أن تُصمم وتُنفذ وتُفحص بشكل دوري لضمان دعمها لمتطلبات كل قانون تشريعي.
	• يحب حماية البيانات ومعالجتها بشكل صحيح طبقاً لكل قانون تشريعي.
التسهيلات (المرافق)	• يجب أن تكون جميع التسهيلات مصممة ومتاحة لتلبية احتياجات كل قانون تشريعي (فعلى سبيل المثال، قد تتطلب بعض القوانين التشريعية بأن تكون السجلات متاحة بكل سهولة وسرعة خارج الموقع).

أهمية ممارسات ومبادئ نموذج GRC الفعالة:

تحتاج المؤسسة إلى الاعتماد على ممارسات وإجراءات قوية لكل من عمليات الحوكمة وإدارة المخاطر والامتثال بهدف إيجاد برنامج فعال لنموذج GRC. فعلى الرغم من أن معظم الفصول اللاحقة تركز على عمليات حوكمة تقنية المعلومات، إلا أننا يجب ألا ننسى أبداً الأهمية الكبرى للعمليات القوية لكل من الحوكمة وإدارة المخاطر والامتثال والتي تقوم بدعم كلٍّ من حوكمة تقنية المعلومات وغيرها من عمليات التشغيل في المؤسسة. سيتم ذكر مبادئ وممارسات نموذج الحوكمة وإدارة المخاطر والامتثال GRC في جميع الفصول القادمة التي تركز أكثر على قضايا محددة في المخاطر والحوكمة.

ومثالاً على ذلك، سيناقش الفصل الخامس عشر من هذا الكتاب أهمية تطبيق نظم متكاملة لحوكمة وإدارة تقنية المعلومات. فهو يناقش الأدوار والمسؤوليات المطلوبة لكلٍ من الأشخاص والإدارات للوصول إلى حوكمة فعالة. كما يحدد أساليب التواصل مع المستويات المختلفة لقواعد الحوكمة. وكذلك الأمر بالنسبة للفصل التاسع عشر من هذا الكتاب، الذي ينظر إلى دور التدقيق الداخلي في حوكمة تقنية المعلومات المؤسسية. حيث يوضح هذا الفصل النهج المتبع في تقييم المخاطر والتخطيط لها من قبل إدارة التدقيق الداخلي لكي تقوم بتحديد قضايا الامتثال الأكثر أهمية بالنسبة لها، ولكي تقوم أيضاً بإيصال تلك القواعد والمبادئ الخاصة بالامتثال للجميع، ولكي تقوم بعد ذلك بمراقبة الأداء الحقيقي لعملية الامتثال في المؤسسة. فهذا الفصل يناقش كيف يمكن للقانون والتدقيق الداخلي أن يساعدوا المؤسسة على تحقيق الامتثال.

على الرغم من أن البرامج القوية لحوكمة تقنية المعلومات تعد من الأمور الهامة للغاية، فإنها يجب أن تكون أيضاً مدعومة من قبل برامج الحوكمة وإدارة المخاطر وكذلك الامتثال الكلي لنموذج GRC. كما يجب على المؤسسة أن تركز على العديد من أنشطتها على مبادئ برنامج GRC بشكل قوي. قدم هذا الفصل بعض المفاهيم المؤسسية العالية المستوى الهامة لبرنامج GRC. فهذه المفاهيم يجب أن تكون من المكونات الأساسية لعمليات حوكمة تقنية المعلومات.

الجزء الثاني
أطر عمل لدعم حوكمة فعالة لتقنية المعلومات

الفصل الرابع
حوكمة تقنية المعلومات ونظم الرقابة الداخلية طبقاً للجنة المنظمات الراعية (كوسو- COSO)

إن الحاجـة إلى نظـم رقابة داخلية قويـة وفعالة تعد عنصراً أساسـياً في حوكمة تقنية المعلومات لأي مؤسسـة. فقد ظهرت الحاجة إلى إنشـاء رقابة داخلية وتقييمها منذ الأيام الأولى لظهـور نظم التدقيق، بل كانت أيضاً قضية مهمة تعود إلى الأيام الأولى لنشـأة نظم تدقيـق تقنية المعلومـات. وفي حين ظهرت تعريفـات عديدة لنظم الرقابـة الداخلية في السـنوات الماضية فإن هناك تعريفاً عاماً جيداً يتناسب مع حوكمة تقنية المعلومات مفاده أن الرقابـة الداخليـة عبارة عن "عمليـة تتأثر بمجلس إدارة كيان مـا وإدارته وغيرهم من الأفراد في ذلك الكيان، ويكون الهدف من تصميمها الحصول على تأكيد معقول حول تحقيق الأهداف المنتظرة من فاعلية العمليات وكفاءتها وموثوقية وضع التقارير المالية للمؤسسـة ونظم وعمليات تقنية المعلومات داخل المؤسسـة، كل ذلك مع الالتزام بالقوانين واللوائح". ويتشابه هذا التعريف مع التعريف المعروف الموضوع من قبل اللجنة الأمريكية للمنظمات الراعيـة (COSO)، وهي هيئة مهمة تقدم توجيهات تتعلق بنظـم الرقابة الداخلية التي سنناقشها لاحقاً في هذا الفصل.

يتحمل مديرو المؤسسة مسئولية تنفيذ عمليات الرقابة الداخلية وإدارتها، في حين يعمل مدققوهم أطرافاً مستقلة تقوم بمراجعة اختبارات نظم الرقابة الداخلية وإجرائها بالإضافة إلى رفع تقارير إلى الإدارة والأطراف الأخرى حال بلوغهم حد الكفاية. ويضم مدققو الرقابة الداخليـة كلاً مـن المدققين الداخليـين والخارجيين، حيث يتبنى المدققـون الخارجيون في الولايات المتحدة معايير التدقيق الخاصة بالمعهد الأمريكي للمحاسبين القانونين (AICPA). وعموماً يشـترك المدققون الداخليون في اتباع إرشـادات معهـد المدققين الداخليين (IIA)، وهـي منظمتهم المهنية الدولية التي سـيتم التطرق إليها في الفصل التاسـع عشر من هذا الكتاب.

لــكل من منظمتي التدقيق هاتين إرثٌ يعود إلى أيام اســتخدام الورقة والقلم الرصاص في التدقيق وحتى قبل ما نشــهده اليوم من الاســتخدام الســائد والاعتــماد على عمليات تقنيــة المعلومات ونُظُمِها. كما قامت جمعيــة تدقيق ومراقبة نظم المعلومات (ISACA) والمتخصصون لديها في مجال تدقيق تقنية المعلومات بتلبية جزء كبير من الحاجة إلى وجود نظم رقابية داخلية فعالة.

يضطلــع مدققو تقنية المعلومات بأدوار التدقيق الداخلي والخارجي، على الرغم من أن غالبية المهنيين هنا يعملون مدققين داخليين لمؤسساتهم.

ومتابعــة منا للمناقشــة التي أجريناهــا في الفصل الثاني عن حوكمــة تقنية المعلومات وقوانين ساربينز-أوكسلي (SOx)، فإننا نقدم في هذا الفصل ما يعرف بإطار الرقابة الداخلية الخــاص بلجنة المنظمات الراعية (COSO) كما يلخص عمليــات حوكمة تقنية المعلومات المرتبطة بهذه اللجنة (COSO) في مؤسسات أعمال عصرنا الحاضر. إن كلاً من نظم الرقابة الداخلية الخاصة بلجنة المنظمات الراعية (COSO) وقوانين ساربينز-أوكسلي (SOx) التي ناقشناها في الفصل الثاني بدأت مجرد قوانين توجيهية لنظم الرقابة الداخلية المعمول بها في الولايات المتحدة، غير أنها قد لاقت قبولاً الآن في جميع أنحاء العالم. فقد كان كل منهما في الأساس عبارة عن توجيهات عامة لمراجعة الشئون المالية وعمليات التشغيل وتقبل التطبيق تماماً في بيئات حوكمة تقنية المعلومات.

إن فهــم إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) واســتخدامه يعــد أمراً هاماً لوضع عمليات فعالــة لحوكمة تقنية المعلومات. ورغــم أن هذه القواعد والإجراءات ترجع أصولها إلى إعداد التقارير المالية وتدقيقها، فإنه في عالم اليوم الذي يرتكز عــلى تقنية المعلومــات تجد أن نظم أو ضوابط الرقابة الداخليــة الخاصة بلجنة المنظمات الراعية (COSO) تعتبر أدوات هامة في حوكمة تقنية المعلومات. وتلك هي القواعد التي تتبناها المؤسســات للتأكيد أو التصديق للجهات الرقابية بــأن منظماتهم تتبع نظماً رقابية داخلية فعالة وأنها تعمل وفقاً لهذه القواعد الجديدة.

أهمية أنظمة الرقابة الداخلية الفعالة ولجنة المنظمات الراعية (COSO):

تعد نظم الرقابة الداخلية أحد المفاهيم الأساسية وأكثرها أهميةً ويجب على كبار المديرين والمهنيين على جميع المستويات أن يفهموها، حيث يقوم المهني بوضع نظم الرقابة الداخلية واستخدامها في حين يقوم المدققون بمراجعة النظم والعمليات التشغيلية والتقنية والمالية واختبارها بهدف تقييم ما لديها من نظم رقابة داخلية. ومع أن كلاً من المدققين الداخليين والخارجيين لديهم أهداف متباينة فإن معظم مرجعياتنا في هذا الفصل تنطبق على كبار المديرين الذين تقع على عاتقهم مسئولية رئيسية لفهم قضايا حوكمة تقنية المعلومات وتقييم نظم الرقابة الداخلية ذات الصلة بتقنية المعلومات.

وعلى الرغم من وجود تعريفات كثيرة مختلفة نسبياً لنظم الرقابة الداخلية في الماضي، فإن إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) الذي سنناقشه في الأجزاء التالية يقدم تعريفاً مناسباً لكبار المديرين، فهذا التعريف يقر بأن الرقابة الداخلية لا تقتصر فقط على الأمور المالية والمحاسبية بل تتعدى هذا الحد لتشمل جميع عمليات المؤسسة. ولأن تقنية المعلومات تمثل أيضاً جزءاً لا يتجزأ من جميع عمليات الأعمال، فإن نظم الرقابة الداخلية ذات الصلة بتقنية المعلومات تعد جزءاً رئيسياً من فهمنا الشامل لنظم الرقابة الداخلية. ويمكن الحكم بأن المؤسسة، في صورة وحدة أو عملية، يكون لها نظم رقابة داخلية جيدة إذا كانت (١) تحقق مهمتها المعلنة بطريقة أخلاقية، (٢) تعطي بيانات دقيقة وموثوقاً بها، (٣) تتوافق مع القوانين المعمول بها ومع سياسات المؤسسة، (٤) توفر استخدامات فعالة واقتصادية لمواردها، وأخيراً (٥) توفر حماية مناسبة للأصول. يتحمل جميع أعضاء المؤسسة المسئولية عن نظم الرقابة الداخلية في مجال عملياتهم التشغيلية وكذا عن تشغيلها على نحو فعال.

وعلى الرغم من - أو بسبب - هذا التعريف الفضفاض لنظم الرقابة الداخلية، فإننا نجد أن كثيراً من المهنيين كانت لديهم مشاكل في فهم مفاهيم الرقابة الداخلية وتطبيقها تماماً. وبالنظر إلى تعريفنا هذا بصورة مختلفة بعض الشيء نجد أن مفهوم الرقابة الداخلية ودعم عمليات الرقابة تعود إلى الإجراءات الآلية والأعمال الورقية الأساسية التي كانت تتم بشكل متكرر في جميع العمليات التجارية اليومية. وتعد أعمال الرقابة ضروريةً للأنشطة داخل

وخارج مؤسسات اليوم، وأن العديد من المفاهيم والمبادئ الأساسية تكون متماثلة بغض النظر عن مكان تطبيق الرقابة. وتقدم السيارة بعض أمثلة على الرقابة الأساسية، فعند الضغط على المُسرِّع - ضابط السرعة - فإن السيارة تسير بشكل أسرع وعند الضغط على المكابح - وهو ضابط آخر للسرعة - فإن السيارة تسير ببطء أو تتوقف، وعندما تُدار عجلة القيادة فإن السيارة تقوم بالدوران، وبذلك يتحكم السائق في السيارة ويمثل كلٌ من هذه الأجزاء الثلاثة النظام الأساسي للرقابة الداخلية بالسيارة. وإذا لم يقم السائق باستخدام المسرع أو المكابح أو عجلة القيادة أو إذا استخدمها بشكل غير ملائم فإن السيارة ستعمل خارج نطاق السيطرة.

وبتوسيع هذا المفهوم قليلاً، فإننا نجد أن إشارات التوقف وإشارات توجيه المرور وحواجز عبور البوابات تمثل جميعها نظم الرقابة الخارجية للسيارة وسائقها، وفي حين أن قائد السيارة هو المشغل لعملية - أو نظام - الرقابة الداخلية بالسيارة، إلا أن سلطة اتخاذ القرار لديه تكون ضعيفة عند التعامل مع الرسالة الموجهة إليه من إشارة ضوئية تمثل الرقابة الخارجية.

ومن منظور الرقابة الداخلية يمكن مقارنة المؤسسة بمثال السيارة الذي ذكرناه. كما سنجد عديداً من نظم وعمليات المؤسسة المفعلة مثل عمليات المحاسبة وعمليات البيع ونظم تقنية المعلومات؛ وإذا لم تقم الإدارة بتشغيل أو توجيه هذه العمليات بشكل صحيح، فإن المؤسسة ربما تعمل خارج نطاق السيطرة. ويتعين على جميع أعضاء المؤسسة بلورة فهم ما لنظم الرقابة المناسبة وتقرر من خلاله ما إذا كانت هذه النظم مرتبطة بشكل صحيح بإدارة المؤسسة. ويشار إلى هذه النظم بمسمى أنظمة الرقابة الداخلية للمؤسسة.

معلومات أساسية عن معايير الرقابة الداخلية:

على الرغم من أن مفهوم الضوابط الداخلية وتعريفها أصبح من السهل اليوم فهمها بشكل جيد فإن هذا الأمر لم يكن صحيحاً حتى أواخر ثمانينيات القرن العشرين. وعلى الرغم من أننا كنا ندرك غالباً المفهوم العام، فإنه لم يتوافر اتفاقٌ ثابتٌ بين العديد من المهنيين المهتمين بالأعمال والمحاسبة فيما يتعلق بالمقصود من "نظم الرقابة الداخلية

الجيــدة". وتتمثــل أمامنا نقطة انطلاق جيــدة لذلك من خلال التعريفــات الأولى التي صــدرت في البداية من المعهد الأمريكي للمحاســبين القانونيين (AICPA) واســتخدمتها هيئــة الأوراق المالية والبورصــة الأمريكية (SEC) تنفيذاً لقانــون بورصة الأوراق المالية الخاص بلوائح عام ١٩٣٤. ومع حدوث تغيرات بمرور السنين، فإن معايير معهد المحاسبين القانونيــين الأمريكيين (AICPA) التي تم تدوينها في البداية وكانت تســمى بيان معايير التدقيــق رقم ١ (SAS No.1)[1] حددت ممارســة التدقيق الخارجــي للبيانات المالية في الولايات المتحدة لسنوات عديدة. وقد تعرض هذا التعريف الذي وضعه المعهد الأمريكي للمحاســبين القانونيين (AICPA) للرقابة الداخلية بالطبــع لتغييرات وتنقيحات على مر الســنين. وخلال هذه الفترة وتحديداً خلال ســبعينيات القرن العشرين ظهرت تعريفات عديــدة للرقابة الداخلية صدرت عــن هيئة الأوراق المالية والبورصــة الأمريكية (SEC) والمعهــد الأمريكي للمحاســبين القانونــين (AICPA) إلى جانب العديد من التفســيرات والإرشادات التي وضعتها وطورتها بعد ذلك كبرى شركات التدقيق الخارجي.

لقد تغيرت الأوضاع في الفترة الأخيرة من ســبعينيات وأوائل ثمانينيات القرن العشرين، تلك الفترة التي شــهدت العديد من الإخفاقات في المؤسســات الأمريكية الكبرى نظراً لعدة عوامل منها ارتفاع معدلات التضخم وارتفاع أسعار الفائدة المصاحبة لذلك. وفي عديد من الوقائع أشــارت الشركات إلى وجود أرباح مناســبة في تقاريرها المالية المُدققة، في حين أنها وبعــد فــترة وجيزة من نشر تلك التقارير المالية المدققــة الإيجابية تتعرض لانهيار مالي. لم تتســبب التقارير المالية الاحتيالية إلا في حدوث القليل من تلك الإخفاقات، في حين حدث أغلبُها بســبب ارتفاع معدلات التضخم أو قضايا أخرى كانعدام الاســتقرار في المؤسســات. وعــلى الرغــم من ذلك، فقد اقترح العديــد من أعضاء الكونجرس الأمريكي ســن تشريع لـ "تصحيــح" الإخفاقــات المحتملة في الأعمال وعمليــات التدقيق، وقد تــم صياغة القوانين وعقدت جلسات الاستماع في الكونجرس لكنها لم تسفر عن تمرير أي تشريع. وللقضاء على هــذه المخاوف ونظراً لعدم وجود إجراء تشريعي، فقد تم تشــكيل اللجنة الوطنية المعنية بدراســة وضع التقارير المالية الاحتيالية. وقد ضمت هــذه اللجنة خمس منظمات مهنية هي: IIA وAICPA وقد سبق ذكرهما؛ ومعهد المديرين التنفيذيين الماليين الدوليين (FEI) وهــي جمعية من كبار المديريــن الماليين؛ وجمعية المحاســبين الأمريكين (AAA)؛ ومعهد

المحاســبين الإداريين (IMA). وتعد جمعية المحاســبين الأمريكيين (AAA) منظمةً مهنيةً تضم المحاسبين الأكاديميين، في حين يمثل معهد المحاسبين الإداريين (AMI) المنظمة المهنية للمحاسبين الإداريين أو محاسبي التكاليف.

وقد سُــميت اللجنة الوطنية المعنية بوضع التقارير الاحتيالية بـ"لجنة تريدواي" نسبة إلى رئيسها، وقد اقتصرت أهداف هذه اللجنة على تحديد العوامل والأسباب التي سمحت بوجود تقاريــر مالية احتيالية وعلى إصدار توصيات من شــأنها الحــد من تكرار حدوثها. وقد صدر التقرير النهائي للجنة تريدواي في عام ١٩٨٧م[٢] وتضمن عدداً من التوصيات للعاملين في الإدارة ومجالس الإدارة وأقســام المحاســبة القانونية العمومية وغيرهم. كما دعــت أيضاً إلى إعداد تقاريــر إدارية عن فاعلية نظــم الرقابة الداخلية لديها والتأكيد على العناصر الرئيســية التي يجــب توافرها في نظام الرقابة الداخلية متضمناً ذلك توافر بيئة رقابة قوية وقواعد ســلوكية ولجــان تدقيق معنية ومختصة وإدارة تدقيق داخلي قوية. وقد أوضح تقرير لجنة تريدواي مرة أخرى عدم وجود تعريف ثابت للرقابة الداخلية، ويشــير بذلك إلى الحاجة إلى مزيد من العمل في المســتقبل. وقد قامت لجنة المنظمات الراعية (COSO) نفســها التي أدارت تقرير تريــدواي بالتعاقد في وقت لاحق مع مختصين مــن الخارج وأطلقت مشروعاً لتعريف الرقابة الداخلية، وعلى الرغم من عدم إصدار اللجنة لأية معايير، فإنها أصدرت إطاراً للرقابة الداخلية خاصاً بها ستتم مناقشته في الأجزاء التالية ويشار إليه عبر فصول هذا الكتاب.

إطار الرقابة الداخلية الذي أصدرته لجنة المنظمات الراعية (COSO):

كما ذكرنا من قبل، يشير مصطلح لجنة المنظمات الراعية (COSO) إلى المنظمات المهنية الخمس العاملة في مجال التدقيق والمحاسبة، تلك المنظمات التي شكلت لجنة لوضع تقرير الرقابة الداخلية المشــار إليه؛ ويحمل مسماه الرسمي "الإطار المتكامل للرقابة الداخلية"[٣]. سنشــير إلى هذا الإطار عبر هذا الكتاب بعبارة "تقريــر أو إطار الرقابة الداخلية" COSO، وهــذا بخلاف إدارة المخاطر المؤسســية للجنة المنظمات الراعيــة (COSO ERM) وإطار إدارة المــوارد الوارد في الفصل الثامن من هذا الكتاب. ومنذ صدور تقرير الرقابة الداخلية للجنة المنظمات الراعية (COSO) للمرة الأولى في سبتمبر ١٩٩٢ اقترُح إطار مشترك لتعريف نظــم الرقابة الداخلية فضلاً عن وضع إجراءات لتقييم هذه النظم الرقابية. وما إن مضت

سنوات قليلة من صدروه عام ١٩٩٢م حتى أصبح هذا الإطار هو الإرشادات المتعارف عليها في جميع أنحاء العالم لفهم ووضع رقابة داخلية فعالة في كل أنظمة الأعمال تقريباً. وتقدم الفقرات التالية وصفاً لإطار الرقابة الداخلية للجنة المنظمات الراعية (COSO) واستخدامه أداة لحوكمة تقنية المعلومات لإجراء تقديرات وتقييمات لنظم الرقابة الداخلية.

يوجد لدى جميع الشركات العامة تقريباً هيكل إجراءات رقابية معقدة، ووفقاً لشكل المخطط التنظيمي التقليدي، قد يكون هناك مستويات إدارية عليا ووسطى في وحدات التشغيل المتعددة أو ضمن الأنشطة المختلفة. وإضافة إلى ذلك، قد تختلف الإجراءات الرقابية نوعاً ما في كل من هذه المستويات والمكونات. فعلى سبيل المثال، يمكن أن تعمل إحدى وحدات التشغيل في بيئة عمل منتظمة تكون فيها العمليات الرقابية مهيكلة تماماً، في حين قد تعمل وحدة أخرى في صورة مشروع ناشئ بهيكل رسمي أقل بكثير. ومن ثم فالمستويات المختلفة للإدارة في هذه المؤسسات سيكون لها رؤى مختلفة عن كيفية التعامل مع نظم الرقابة. وإذا ما تساءلنا هنا "كيف تصف نظام الرقابة الداخلية الخاص بك؟" فإننا سنتلقى إجابات مختلفة من أشخاص من مختلف المستويات أو من وحدات كل من هذه المكونات المؤسسية.

وتقدم لنا لجنة المنظمات الراعية (COSO) وصفاً ممتازاً لهذا المفهوم متعدد الأبعاد لنظم الرقابة الداخلية، حيث وضعت تعريفاً للرقابة الداخلية كما يلي:

الرقابة الداخلية هي عملية يقوم على تنفيذها مجلسُ إدارة كيانٍ معين وإدارةٌ وغير ذلك من الأفراد ويتم تصميمها لتعطي تأكيداً معقولاً فيما يتعلق بإنجاز الأهداف في النواحي التالية:

- فاعلية وكفاءة عمليات التشغيل.
- مصداقية وضع التقارير المالية.
- الالتزام بالقوانين واللوائح المعمول بها[٤].

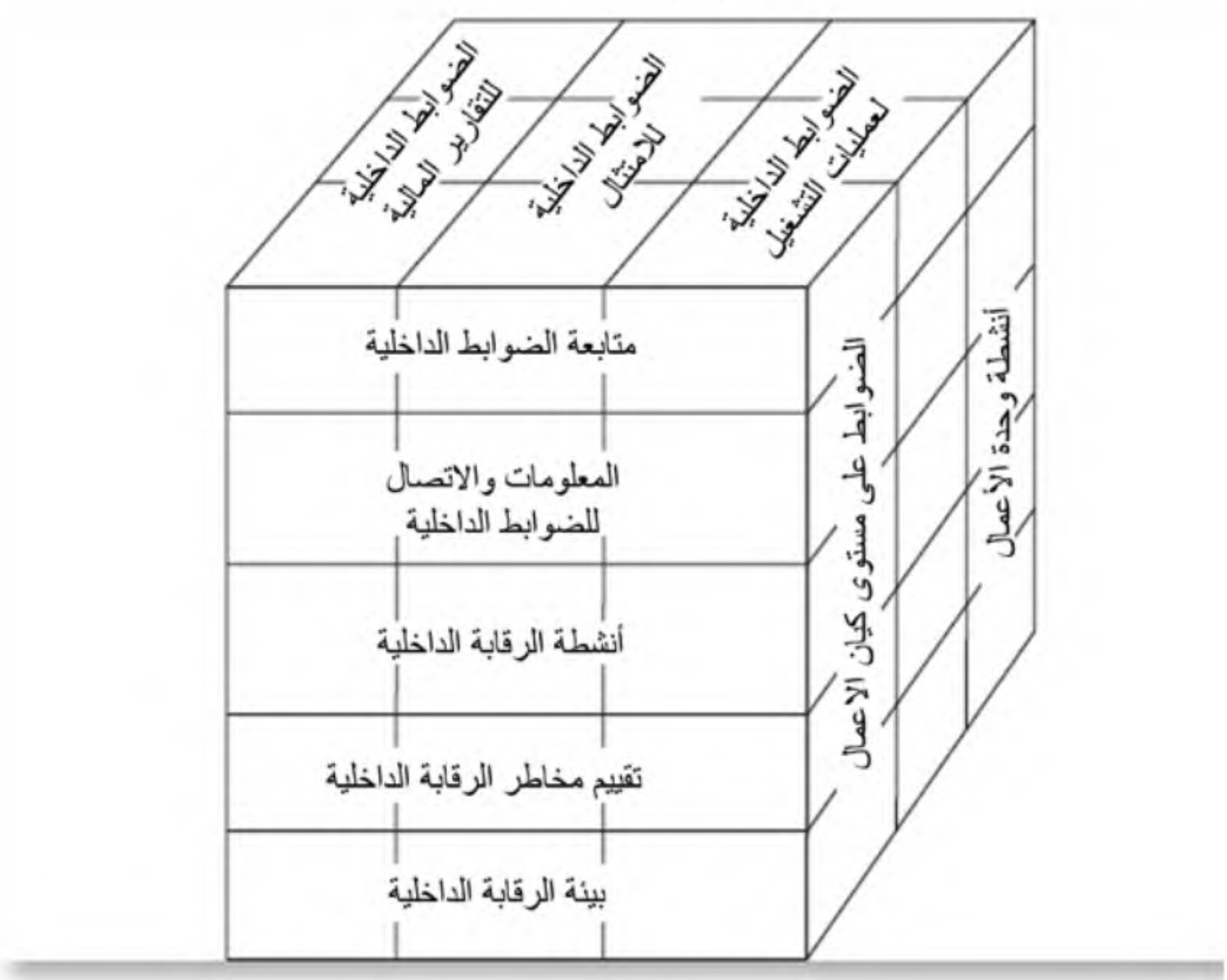
وللاستفادة من هذا التعريف الأشمل للرقابة الداخلية تستخدم لجنة المنظمات الراعية (COSO) نموذجاً أو إطاراً ثلاثي الأبعاد لوصف نظام الرقابة الداخلية في المؤسسة.

ويبين الشــكل التوضيحي (٤-١) إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) على أنها نموذج ثلاثي الأبعاد بمســتويات خمسة على الجانب المواجه من الشكل والمكونات الثلاثة الرئيســية للرقابة الداخلية - وهي فاعلية العمليات التشــغيلية وكفاءتها وموثوقية التقارير المالية والالتزام بالقوانين واللوائح المعمول بها - تأخذ قطاعات متساوية إلى حد ما من النموذج في شــكل شرائح عبر قمته، ويُبين الجانب الأيمن من الشــكل ثلاثة أقسام، ومع ذلك قد يوجد عديدٌ من هذه الأقسام تبعاً لبنية المؤسسة.

كما أن كل مســتوى من مســتويات الجهة الأمامية من إطار الرقابــة الداخلية الخاص بلجنــة المنظمات الراعية (COSO)، بدءاً من المتابعة في القمة ونزولاً إلى بيئة نظم الرقابة الداخلية، سوف تتم مناقشته بمزيد من التفاصيل في الأقسام التالية.

شكل توضيحي (٤-١)

إطار الرقابة الداخلية COSO



وتـدور الفكرة هنا حول أنه عندما ننظر إلى طبقة أنشـطة الرقابة الداخلية في وسـط النموذج - مثل الإقفال المالي في نهاية السـنة المالية - فإنه يتعين علينا أن نعتبر أن الرقابة فيما يتعلق بوحدة الأعمال أو المؤسسة أو الأقسام المتعددة على جانب الإطار تعمل حيث يتـم تثبيت هذا الضابـط الرقابي. ومع ذلك، ففي هذا النموذج ثـلاثي الأبعاد نجد أن كل ضابط رقابي مرتبطٌ بجميع الضوابط الأخرى في الصف نفسه أو الحزمة أو العمود.

إن الهـدف من إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) يتمثل في أنه ينبغي علينا دائماً أن ننظر إلى كل عنصر من عناصر الرقابة الداخلية الذي تم تعريفه طبقاً لمدى ارتباطه بعناصر الرقابة الأخرى المقترنة به في الإطار ثلاثي الأبعاد. ففي مثالنا عن نظم الرقابة الداخلية الخاصة بالإقفال المالي في نهاية السـنة المالية، يتعين على المؤسسة أن تحتفظ بروابط معلومات واتصالات متعلقة بعمليات الحساب الختامي، كما يجب متابعة النظـام الرقـابي. وبالنزول إلى المسـتوى التالي، نجد ضرورة وجود أنشـطة لتقييم المخاطر مصاحبـة لعملية الرقابة المالية التي يجب أن تعمل في بيئة رقابة داخلية مناسـبة، كما قد يكون للقضايا المتعلقة بعمليات التشـغيل والامتثال عوامـل مؤثرة في النظام الرقابي المتبع الذي قد يعمل على أي مستوى من الهيكل التنظيمي للمؤسسة.

وبينما تصف الأقسـام التالية إطار الرقابة الداخلية للجنة المنظمات الراعية (COSO) بمزيـد من التفصيل، فإنه يجب على كبار المديرين في المؤسسـة فهم إطار الرقابة الداخلية للجنـة المنظمات الراعيـة (COSO) فهماً دقيقاً وكذلك أثـره في حوكمة تقنية المعلومات، وبغـض النظر عن المجال قيـد المراجعة يجب على كبار المديرين دائماً مراجعة نظم الرقابة الداخلية لديهم وتبنيها باعتبارها من هذا النوع متعدد المسـتويات وثلاثي الأبعاد. وتقوم الأقسـام التالية بوصف إطار الرقابة الداخلية للجنة المنظمات الراعية (COSO) بمزيد من التفاصيل، وذلك ابتداء من أول مستوى للجهة الأمامية من الإطار أو من أسفله.

بيئة الرقابة:

يُقصد بالأسـاس أو المستوى السـفلي من إطار الرقابة الداخلية للجنة المنظمات الراعية (COSO) ما تطلق عليه لجنة المنظمات الراعية (COSO) اسم بيئة الرقابة الداخلية.

وينبغي اعتبار بيئة الرقابة الداخلية أساساً لجميع مكونات الرقابة الداخلية الأخرى، كما أن له تأثيراً في كل من الأهداف الثلاثة وأنشطة الوحدة والمؤسسة بكاملها. كما تعكس بيئة الرقابة الداخلية التصور العام والوعي والتصرفات والأفعال من قبل مجلس الإدارة والإدارة وغيرهم بشأن أهمية نظم الرقابة الداخلية في المؤسسة. وبينما يوجد العديد من المفاهيم الأساسية هنا، فإن كل مؤسسة سيكون لديها أساس رقابة داخلية فريدٌ خاصٌ بها.

ويقوم تاريخ المؤسسة وثقافتها غالباً بالدور الرئيسي في تكوين بيئة الرقابة الداخلية هذه. فعندما يكون للمؤسسة إدارةٌ قويةٌ على مدار تاريخها تشدد على تقديم منتجات خالية من العيوب، وعندما تقوم الإدارة العليا بالترويج لأهمية وجود منتجات عالية الجودة إلى كل مستويات المنظمة، فإن ذلك يصبح عاملاً رئيسياً في بيئة الرقابة المؤسسية. كما أن الرسائل التي تأتي من الرئيس التنفيذي (CEO) أو من غيره من كبار مديري المؤسسة تعرف بـ "النغمة السائدة"؛ رسائل الإدارة لجميع أصحاب المصلحة. أما إذا كانت سمعة الإدارة العليا أنها "تتغاضى" عن انتهاكات سياسة المؤسسة، فإن هذا النوع نفسه من الرسائل السلبية سوف يصل بالمثل إلى المستويات الأخرى في المؤسسة. إن النغمة الإيجابية السائدة لدى الإدارة العليا تعد عنصراً أساسياً لبيئة رقابة مؤسسية قوية، سواء لعمليات تقنية المعلومات أو لجميع الأنشطة الأخرى.

ويجب على كبار المديرين أن يحاولوا دائماً إدارة بيئة الرقابة الشاملة في منظماتهم وفهمها، وتصف الفقرات التالية المكونات الأساسية لبيئة الرقابة.

النزاهة والقيم الأخلاقية:

إذا قامت المؤسسة بوضع قواعد سلوكية قوية تشدد على النزاهة والقيم الأخلاقية، وإذا ظهر التزام أصحاب المصلحة بتلك القواعد، فسيكون لدى أصحاب المصلحة جميعهم ما يكفي من الضمانات التي تفيد احتفاظ المؤسسة بمجموعة جيدة من القيم. إن مدونة القواعد الأخلاقية أو السلوكية، كما نوقشت في الفصل العشرين من هذا الكتاب، تعد مكوناً هاماً من مكونات الحوكمة المؤسسية وحوكمة تقنية المعلومات.

وعلى كل حال، حتى وإن كان لدى المؤسسة قواعد سلوكية قوية، فإن مبادئها غالباً ما قد تنتهك بسبب الجهل وليس بسبب المخالفات المتعمدة من قبل الموظف. ففي كثير من الأحيان، قد لا يدرك الموظفون أنهم يرتكبون خطأً أو قد يعتقدون خطأً أن أفعالهم تصب في مصلحة المؤسسة. هذا الجهل ينتج غالباً عن ضعف التوجيه المعنوي من قبل الإدارة العليا أكثر من كونه ناتجاً عن نية الغش من قبل الموظف، وأنه يلزم نقل سياسات المؤسسة وقيمها إلى جميع مستوياتها. وبينما قد يوجد "فاسدون" غالباً في أي مؤسسة، فإن الرسائل المعنوية القوية سوف تشجع الجميع على العمل بشكل سليم، وينبغي أن يكون الهدف دائماً نقل الرسائل أو الإشارات المناسبة إلى جميع أنحاء المؤسسة.

يتعين على أصحاب المصلحة جميعهم، وخصوصاً كبار المديرين، أن يفهموا بشكل جيد مدونة قواعد السلوك وكيفية تطبيقها. وإذا لم تعد القواعد الحالية مناسبةً للزمن أو لا يبدو أنها تعالج قضايا أخلاقية هامة تواجه المؤسسة أو لا يبدو أن المؤسسة قادرة على نقل هذه القواعد إلى أصحاب المصلحة بصورة منتظمة، فإن الإدارة تكون في حاجة إلى أن "تنشط" وتصحح هذا القصور. وبينما تصف مدونة قواعد السلوك قواعد السلوك الأخلاقي، وأنه يتعين على الإدارة العليا أن تنقل الرسالة الأخلاقية السليمة في جميع أنحاء المؤسسة؛ نجد أن الحوافز والإغراءات الأخرى يمكن أن تؤدي إلى تآكل هذه البيئة الرقابية الشاملة، كما قد يميل بعض الأفراد إلى الانخراط في أعمال غير شريفة أو غير قانونية أو غير أخلاقية إذا أعطتهم مؤسساتهم حوافز أو إغراءات لعمل ذلك. على سبيل المثال، قد تقوم المؤسسة بوضع أهداف أداء غير واقعية ومرتفعة جداً للمبيعات أو حصص الإنتاج، فإذا كانت هناك مكافآت ضخمة لتحقيق أهداف الأداء تلك، أو ما هو أسوأ كوجود تهديدات قوية تنذر بفقد الأهداف؛ فإن ذلك قد يشجع الموظفين على المشاركة في الممارسات الاحتيالية أو المشكوك فيها لتحقيق تلك الأهداف.

الالتزام بالكفاءة:

يمكن أن تتآكل البيئة الرقابية للمؤسسة بشكل خطير إذا وظفت عدداً كبيراً من الأشخاص ممن يفتقدون المهارات الوظيفية المطلوبة. وهنا تظهر حاجةُ المؤسسة لتحديد مستويات الكفاءة المطلوبة لمهام الوظائف المتنوعة بها وكذا ترجمة هذه المتطلبات إلى مستويات

ضرورية من المعرفة والمهارة. فعند وضع الأشخاص المناسبين في الوظائف المناسبة وتدريبهم بالشكل المناسب إذا تطلب الأمر ذلك، فإن المؤسسة تكون قد حققت بذلك مكوناً مهماً للبيئة الرقابية طبقاً لإطار (COSO).

مجلس الإدارة ولجنة التدقيق:

تتأثر بيئة الرقابة بشكل كبير بأعمال مجلس إدارة المؤسسة ولجنة التدقيق فيها، فوجود مجلس إدارة فعَّال ومستقل يعد مكوناً أساسياً لبيئة الرقابة الخاصة بلجنة المنظمات الراعية (COSO). ومن خلال وضع سياسات رفيعة المستوى ومراجعة السلوك العام للشركة. يتحمل مجلس إدارة المؤسسة ولجنة التدقيق فيها المسؤولية المطلقة لتحديد "النغمة السائدة" داخل المؤسسة.

فلسفة الإدارة ونمط التشغيل:

إن فلسفةَ الإدارة العليا ونمط التشغيل الذي تعمل به له تأثير كبير في البيئة الرقابية للمؤسسة، فبعض مديري الإدارة العليا في كثير من الأحيان يتحملون مخاطر كبيرة في مشاريع أعمالهم أو منتجاتهم الجديدة، في حين يكون غيرهم حذرين جداً أو متحفظين.

ويبدو أن بعض المديرين يعملون وفق أهوائهم، في حين يصر غيرهم على ضرورة الموافقة السليمة على كل إجراء وتوثيقه كما ينبغي. كما قد يتبنى البعض نهجاً قاسياً في تفسيراتهم للقواعد الضريبية وإعداد التقارير المالية، في حين أن البعض الآخر يتبع التعليمات بدقة. ولا تعني هذه التعليمات بالضرورة أن نهجاً معيناً جيدٌ والآخر سيئ على طول الخط.

إن هذه الاعتبارات الخاصة بفلسفة الإدارة والنمط التشغيلي تمثل جميعها جزءاً من بيئة الرقابة للمؤسسة. وفي حين أنه لا توجد مجموعةٌ واحدةٌ من الأنماط والفلسفات تكون هي الأفضل لجميع المؤسسات، فإن هذه العوامل تكون مهمة عند دراسة المكونات الأخرى للرقابة الداخلية وممارسات حوكمة تقنية المعلومات في مؤسسة ما.

الهيكل التنظيمي:

يوفـر مكون الرقابة الداخلية هذا إطاراً لأنشـطة التخطيط والتنفيـذ والرقابة والمتابعة للمسـاعدة في تحقيق الأهداف العامة للمؤسسة. إن عامل بيئة الرقابة هذا يتعلق بكيفية إدارة الوحدات أو الإدارات وتنظيمها. ومع أن الهيكل التنظيمي يمثل جانباً مهماً من جوانب البيئة الرقابية للمؤسسة، فإنه لا يوجد هيكلٌ معينٌ يقدم لنا بيئةً رقابيةً داخليةً مفضلةً.

إن الهيـكل التنظيمي هو الطريقة أو النهج الموضوع لجهـود العمل الفردي التي يلزم تخصيصها وتكاملها بهدف تحقيق الأهداف العامة. فكل مؤسسـة تحتاج إلى خطة فعالة لتنفيذ هذا الهيكل التنظيمي، لكن ضعف نظم الرقابة في المنظمة قد يؤثر بشـكل كبير في البيئة الرقابية بأكملها. وعلى الرغم من الخطوط الواضحة للسلطة، فإن المؤسسات في كثير من الأحيان تعاني بعض أوجه القصور الداخلية التي يمكن أن تزيد كلما اتسعت المؤسسات بمرور الوقت، الأمر الذي يتسبب في حدوث خلل في إجراءات الرقابة.

تخصيص السلطة والمسئولية:

يتشـابه هذا الجانب من بيئة الرقابة مع مكون الهيكل التنظيمي الذي سـبق مناقشـته، ويحدد الهيكل التنظيمي للمؤسسة تخصيص إجمالي جهود العمل في المؤسسة وتكاملها. ويمثل تخصيص الصلاحية في الأسـاس الطريقة التي يتم بها تحديد المسئوليات من حيث التوصيف الوظيفي ويتم صياغتها طبقاً لمخططات المؤسسة. وعلى الرغم من أن المهام الوظيفية لا يمكن أن تخلو تماماً من بعض المسـئوليات المتداخلة، فإنه كلما كان بيان هذه المسئوليات أكثر دقة كان ذلك أفضل. إن الإخفاق في وضع تعريف واضح لصلاحية ومسئولية محل العمل يتسبب غالباً في الالتباس والتعارض بين جهود العمل الفرديةً والجماعية.

سياسات وممارسات الموارد البشرية:

تشـمل ممارسـات الموارد البشرية توظيف وتوجيه وتدريب وتقييـم العاملين وكذلك تقديم المشـورة لهم وترقيتهم ومكافأتهم واتخاذ الإجراءات الإصلاحية المناسـبة بشـأنهم. وبينما يتعين على إدارة الموارد البشرية الاحتفاظ بسياسـات معلنة ومواد إرشـادية ملائمة وكافية، فإن ممارساتها الفعلية تبعث برسائل قوية للموظفين عن المستويات المتوقعة لتوافق

الرقابة الداخلية والسلوك الأخلاقي والاختصاص. إن الموظف الأعلى الذي يتجاهل أو ينتهك صراحةً سياسة إدارة الموارد البشرية سرعان ما يبعث رسالة بما ارتكب إلى المستويات الأخرى في المؤسسة، ويزداد صدى هذه الرسالة بشكل أكبر خصوصاً عندما ينال موظفٌ أدنى عقوبة تأديبية لانتهاكه السياسة نفسها في حين يغض الجميع الطرف عن المخالف الأعلى.

تعد سياسات إدارة الموارد البشرية وإجراءاتها الفعالة مكوناً بالغ الأهمية في بيئة الرقابة الخاصة بلجنة المنظمات الراعية (COSO) بكاملها. ولن تحقق الرسـائل الواردة من قمة الهيكل القوي للمؤسسة إلا القليل إذا انعدم لدى المؤسسة إجراءات وسياسات قوية لإدارة الموارد البشرية.

خلاصة القول: كما أن الأساس المتين أمرٌ ضروريٌ لإنشاء مبنى متعدد الطوابق، فإن بيئة الرقابة تعد أساس المكونات الأخرى للرقابة الداخلية. إن المؤسسة التي تريد أن تنشئ بنية رقابة داخلية قوية ينبغي عليها أن تُولي اهتماماً خاصاً لوضع حجر أسـاس صلب في أسـاس بيئـة الرقابة تلك. إن بيئة الرقابة الداخليـة الخاصة بلجنة المنظمات الراعية (COSO) لا تتطلب مجرد مجموعة قواعد من نوعية "هل يتساوى الدائنون مع المدينون" لكنها تحتاج إلى سياسات قوية وفعالة وشاملة على مستوى المؤسسة.

تقييم المخاطر:

إن المستوى التالي - أو الطبقة التي تعلو مستوى بيئة الرقابة في إطار الرقابة الداخلية للجنة المنظمات الراعية (COSO) - يمثل مسـتوى تقييم المخاطر. إن قدرة المؤسسـة عـلى تحقيق أهدافها يمكن أن تكون عرضة للمخاطر بسـبب وجود نوعية من العوامل الداخلية والخارجية. كما أن فهم بيئة المخاطر وإدارتها يمثل عنصراً أساسـياً في تأسـيس الرقابـة الداخلية ويجب أن تباشر المؤسسـة إجراءات تُقيّم من خلالها المخاطر المحتملة التـي قد تؤثر في تحقيق أهدافها المتنوعة. ويركز مكون تقييم المخاطر هذا على الرقابة الداخلية داخل المؤسسة، ويكون تركيزه أضيق بكثير من تركيز إطار إدارة مخاطر المؤسسة (COSO ERM) وقضايـا إدارة مخاطر حوكمة تقنية المعلومات التي تتم مناقشـتها في الفصل الثامن من هذا الكتاب.

وينبغــي أن يكون تقييــم مخاطر الرقابة الداخلية للجنــة المنظمات الراعية (COSO) عملية اســتشرافية يتم تنفيذها على جميع المســتويات وبشكل فعلي على جميع الانشطة داخل المؤسســة. ويصف إطار الرقابة الداخليــة للجنة المنظمات الراعية (COSO) تقييم المخاطر على أنها عملية من ثلاث خطوات:

١- تقدير تأثير المخاطرة.

٢- تقييم احتمال أو تكرار حدوث المخاطرة.

٣- البحث في كيفية إدارة المخاطرة كما ينبغي وتقييم الإجراءات التي يجب اتخاذها.

إن عملية تقييم المخاطرة الخاص بلجنة المنظمات الراعية (COSO) تُلقي بالمســئولية عــلى الإدارة لتقييم ما إذا كانت المخاطرة مؤثــرة، فإن كان الأمر كذلك، فعلى الإدارة اتخاذ الإجراءات المناسبة.

كما تؤكد الرقابة الداخلية الخاصة بلجنة المنظمات الراعية (COSO) أن تحليل المخاطر ليس عملية نظرية، ولكنه في كثير من الأحيان قد يكون حاســماً في تحقيق النجاح الشــامل للكيان المؤســسي. ويجب على الإدارة، بوصفها جزءاً من التقييم الشــامل الذي تجريه على الرقابة الداخلية، أن تتخذ الخطوات اللازمة لتقييم المخاطر التي قد تؤثر في المؤسســة كلها فضلاً عن المخاطر التي تدور حول مختلف أنشــطة المؤسســة وكياناتها. وتوجد نوعية من المخاطر، تنتج عن عوامل داخلية أو خارجية، قد تؤثر في المؤسسة بشكل عام.

إن عنــصر تقييم المخاطر الخاص بلجنة المنظــمات الراعية (COSO) هو المجال الذي يدور حوله الكثير من اللغط والبلبلة بســبب تشابه مسماه مع إطار إدارة المخاطر الخاص بلجنــة المنظــمات الراعية (COSO ERM) الذي تتم مناقشــته في الفصل الثامن من هذا الكتــاب. إن مكون تقييم المخاطر لإطار الرقابــة الداخلية الخاص بلجنة المنظمات الراعية (COSO) يشــتمل على تقييمات للمخاطر داخل مؤسسة فردية، في حين يشمل إطار إدارة المخاطر الخاص بلجنة المنظمات الراعية (COSO ERM) الكيان المؤسسي بأكمله وخارجه. وفي واقع الأمر، هاتان قضيتان منفصلتان؛ وأحدهما لا يصح أن يكون بديلاً عن الآخر.

أنشطة الرقابة:

تسمى الطبقة التالية من إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) أنشطة الرقابة وتمثل العمليات والإجراءات التي تساعد على ضمان تنفيذ الأعمال المخصصة لمعالجة المخاطر. وتوجد أنشطة الرقابة على جميع المستويات، وفي كثير من الحالات قد يتداخل بعضها مع بعض. وهي عناصر ضرورية لبناء ثم ترسيخ نظم رقابة داخلية فعالة في المؤسسة.

يحدد إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) سلسلة من هذه الأنشطة التي يمكن تصنيفها بشكل عام دليلاً إرشادياً أو تقنية معلومات أو نظم رقابة إدارية، كما يمكن توصيفها من منظور كونها أنشطة وقائية أو تصحيحية أو كاشفة. وعلى الرغم من عدم وجود مجموعة تعريفات للرقابة الداخلية تكون صالحة لجميع الأحوال، فإن نظم الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) توصي بأنشطة الرقابة التالية للمؤسسة:

- مراجعات المستوى الأعلى:

يتعين على الإدارة العليا مراجعة نتائج أدائها ومقارنة تلك النتائج بالميزانيات والإحصاءات التنافسية وغيرها من مقاييس المقارنة المرجعية. ومما يمثل هنا أنشطة رقابية تلك الإجراءات التي تتخذها الإدارة لمتابعة نتائج مراجعات المستوى الأعلى ولاتخاذ إجراءات تصحيحية.

الإدارة الفنية أو الوظيفية المباشرة:

يجب على المديرين على مختلف مستوياتهم مراجعة التقارير التشغيلية الصادرة من أنظمتهم الرقابية واتخاذ الإجراءات التصحيحية بالشكل المناسب. ويوجد لدى العديد من أنظمة الإدارة تقارير استثنائية تغطي تلك الأنشطة الرقابية. فعلى سبيل المثال، ضرورة وجود آلية في نظام أمن تقنية المعلومات للإبلاغ عن محاولات الوصول غير المصرح به، وضرورة أن يصاحب ذلك نشاطٌ رقابيٌ يقوم بمتابعة هذه الأحداث المبلغ عنها واتخاذ الإجراءات التصحيحية المناسبة. ويرتبط بعض هذه الأنشطة ارتباطاً وثيقاً بأفضل ممارسات مكتبة البنية التحتية لتقنية المعلومات التي تتم مناقشتها في الفصل السادس من هذا الكتاب.

معالجة المعلومات:

تحتوي نظم تقنية المعلومات غالباً على نظم رقابة للتحقق من التوافق في مجالات معينة ثم الإبلاغ عن أي استثناءات في الرقابة الداخلية. وينبغي أن تُقابل هذه البنود الاستثنائية بإجراء تصحيحي من خلال إجراءات مؤتمتة للنظم أو موظفي التشغيل أو الإدارة. وتشمل أنشطة الرقابة الأخرى نظم رقابة على تطوير نظم جديدة أو على الوصول إلى ملفات البيانات والبرامج.

نظم الرقابة المادية:

من الضروري احتفاظ المؤسسة بنظم رقابة مناسبة على أصولها المادية متضمناً ذلك التجهيزات والمخزون والأوراق المالية القابلة للتداول. ويمثل هنا البرنامج الفعال للجرد المادي الدوري نشاطاً رئيسياً من أنشطة الرقابة، كما أن تقنية المعلومات والتدقيق الداخلي يمكن أن يلعبا دوراً كبيراً في متابعة مدى الامتثال.

مؤشرات الأداء:

ينبغي على الإدارة ربط مجموعات البيانات التشغيلية والمالية بعضها ببعض واتخاذ الإجراءات التحليلية أو الاستقصائية أو التصحيحية المناسبة. وتمثل هذه العملية نشاطاً رقابياً هاماً للمؤسسة يمكن أن يلبي أيضاً متطلبات إعداد التقارير المالية والتشغيلية.

الفصل بين المهام:

يجب تقسيم المهام أو فصلها بين مختلف الأفراد للحد من مخاطر حدوث خطأ أو إجراءات غير لائقة. ويعد هذا إجراءاً رقابياً داخلياً أساسياً يلزم وجوده تقريباً على شاشة رادار كل مدير أعلى.

ولا تمثل هذه الأنشطة الرقابية سوى عدد قليل من الأنشطة الكثيرة التي يتم مباشرتها ضمن السياق المعتاد للعمليات التشغيلية للأعمال، لكنها تتضمن السياسات التي تؤسس لما يجب القيام به والإجراءات اللازمة لتنفيذها. وعلى الرغم من أن أنشطة الرقابة قد يتم الإبلاغ بها شفوياً في بعض الأحيان، فإنه ينبغي تنفيذها بشكل مدروس وبأمانة واستمرارية،

وهذه رسالةٌ قويةٌ لمراجعة أنشطة الرقابة الداخلية تلك. وبالرغم من أن المؤسسة قد تكون صاحبة سياسة معلنة تغطي مجالاً معيناً، فإنه ينبغي أن يكون هناك إجراءات رقابة داخلية ثابتة لدعم هذه السياسة. وقد تكون هذه الإجراءات قليلة القيمة ما لم يكن هناك تركيز حاد على الحالة التي تُوَجه إليها هذه السياسة. وفي أغلب الأحيان قد تنشئ المؤسسة تقريراً استثنائياً كجزء من نظام آلي يتلقى من خلاله المستفيدون أكثر من مجرد المراجعة السطحية بقليل. إلا أنه، وفقاً لأنواع الحالات المبلغ عنها، يجب أن تتلقى تلك الاستثناءات المبلغ عنها إجراءات متابعة ملائمة قد تتنوع تبعاً لحجم المؤسسة والنشاط الوارد في التقرير الاستثنائي.

ويجب أن تكون هذه الأنشطة الرقابية مرتبطة ارتباطاً وثيقاً بعضها ببعض بهدف تحديد المخاطر حسب عنصر تقييم المخاطر لإطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO). كما يجب على كبار المديرين دائماً أن يتذكروا أن الرقابة الداخلية ما هي إلا مجرد عملية وأن أنشطة الرقابة الملائمة يجب أن تُعتمد لمعالجة المخاطر المحددة. ولا يلزم اعتماد أنشطة الرقابة فقط لأنها تبدو "الشيء الصحيح الذي ينبغي عمله"، حتى إذا لم تكن هناك مخاطر كبيرة في المنطقة التي يتم فيها اعتماد النشاط الرقابي. وفي بعض الأحيان، قد تُعتمد أنشطةٌ رقابيةٌ تكون ربما عالجت ذات مرة بعض مخاوف مخاطر الرقابة، على الرغم من أن هذه المخاوف قد تلاشت إلى حد كبير. ولا ينبغي تجاهل نشاط الرقابة لمجرد عدم وقوع أي مخالفة رقابية سابقة، لكن الرقابة تحتاج وبشكل دوري إلى إعادة تقييم للمخاطر النسبية المرتبطة بها. وينبغي أن تسهم جميع أنشطة الرقابة الداخلية في الهيكل الرقابي بشكل عام. كما يجب على مدققي تقنية المعلومات أن يضعوا هذا المفهوم في الاعتبار عند قيامهم بمراجعة الرقابة الداخلية وتقديم التوصيات. ويؤكد إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) على أن إجراءات الرقابة ضرورية لجميع نظم تقنية المعلومات الهامة: المالية والتشغيلية والمرتبطة بالامتثال. وتُقَسِم نظم الرقابة الداخلية (COSO) ضوابط نظم المعلومات إلى ضوابط عامة وضوابط تطبيقات معترف بها. وتنطبق الضوابط العامة على الكثير من إدارات نظم المعلومات للمساعدة في التأكد من توافر إجراءات رقابية كافية على جميع التطبيقات. فقفل الأمان المادي المثبت على باب مركز خوادم تقنية المعلومات يُعتبر مثالاً على الرقابة العامة لجميع

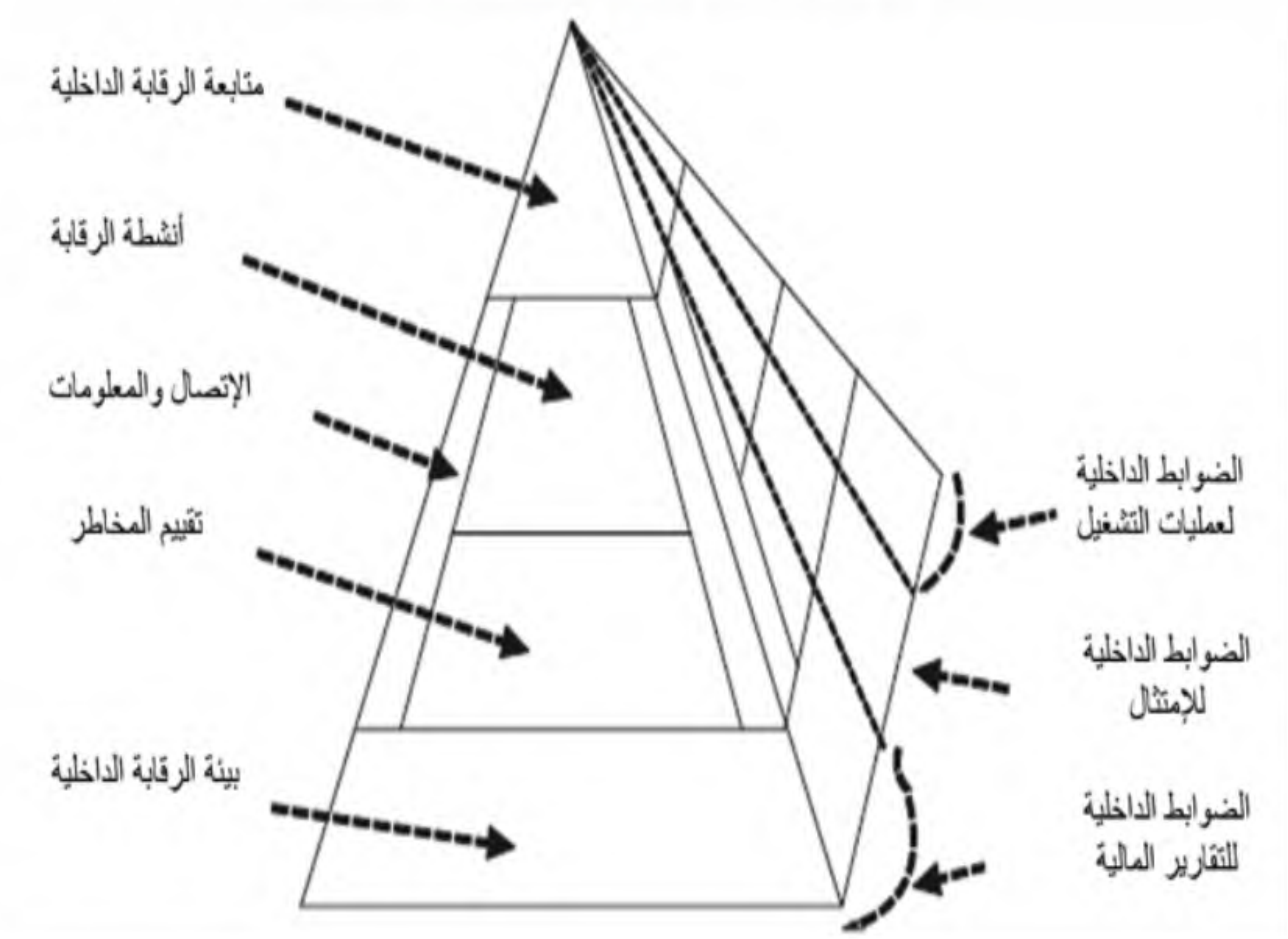
التطبيقات التي تعمل داخل المرفق. وتتم مناقشة الضوابط العامة على تقنية المعلومات في الفصل السادس. كما أن ضوابط التطبيقات التي تتم مناقشتها في الفصل العاشر من هذا الكتاب تمثل أيضاً مجالات رقابة مهمة على تقنية المعلومات لتقييم مدى كفاية نظم الرقابة الداخلية بأكملها. وتُختتم وثيقة إطار الرقابة الداخلية (COSO) بإجراء مناقشة حول ضرورة النظر في تأثير التقنيات المتطورة التي يجب أخذ تأثيرها في الحسبان دائماً عند تقييم أنشطة رقابة تقنية المعلومات. ونظراً لسرعة إدخال تقنيات جديدة فما هو جديد اليوم سرعان ما يحل محله شيء آخر.

الاتصالات والمعلومات:

يصف إطار الرقابة الداخلية (COSO) في الشكل التوضيحي (٤-١) معظم المكونات في شكل طبقات، واحدة فوق الأخرى، بدءاً من بيئة الرقابة باعتبارها الأساس. وهناك طريقة أخرى يُنظر من خلالها للإطار وهي أن تتصور إطار الرقابة الداخلية (COSO) على أنها نموذج هرمي لا تمثل فيه مكونات المعلومات والاتصالات طبقة أفقية، بل عنصراً جانبياً يمتد عبر المكونات الأخرى. وترتبط الاتصالات والمعلومات بعضها ببعض نظراً لكونها أجزاء مهمة في إطار الرقابة الداخلية، إلا أنهما يمثلان في ذات الوقت مكونات رقابية داخلية يتميز بعضها عن بعض. كما يجب نقل المعلومات المدعومة من نظم تقنية المعلومات إلى أعلى المؤسسة وأسفلها بأسلوب وإطار زمني يسمح للأشخاص بتنفيذ المهام الموكلة إليهم. وبالإضافة إلى أنظمة الاتصالات الرسمية وغير الرسمية، يجب أن يكون لدى المؤسسات إجراءات فعالة تعمل على تنفيذها للتواصل مع الأطراف الداخلية والخارجية. وكجزء من أي تقييم للرقابة الداخلية يلزم فهم تدفقات المعلومات والاتصالات والعمليات المرتبطة بها داخل المؤسسة. (انظر الشكل التوضيحي ٤-٢).

شكل توضيحي (٤-٢)

المكونات الأساسية لإطار الرقابة الداخلية COSO



وتحتاج المؤسسة إلى معلومات على جميع المستويات لتحقيق أهدافها التشغيلية والمالية والأهداف المرتبطة بمدى الامتثال. فعلى سبيل المثال، تحتاج المؤسسة إلى معلومات لإعداد التقارير المالية لتقديمها للمستثمرين الخارجيين، فضلاً عن التكلفة الداخلية ومعلومات عن تفضيلات السوق الخارجية لاتخاذ قرارات تسويقية صحيحة. ويلزم أن تتدفق هذه المعلومات من المستويات العليا للمؤسسة إلى المستويات الدنيا وكذلك من المستويات الدنيا إلى المستويات العليا عائدة. وتتخذ الرقابة الداخلية (COSO) نهجاً واسعاً لمفهوم نظام المعلومات مع الاعتراف بأن هذه الأنظمة يمكن أن تكون يدوية، آلية، أو حتى مفاهيمية. كما أن أياً من نظم المعلومات هذه يمكن أن تكون رسمية أو غير رسمية. كما أن المحادثات المنتظمة مع العملاء أو الموردين يمكن أن تكون مصادر معلومات مهمة جداً وتعتبر نوعاً

غير رســمي من نظم المعلومات. ويتعين على المؤسسة الفعالة أن تحتفظ بنظم معلومات تســتخدمهًا للاســتماع إلى طلبات العملاء أو الشــكاوى وإحالة تلك المعلومات التي يبديها العميل إلى الموظفين المناسبين.

كما تؤكد الرقابة الداخلية (COSO) أهمية الاحتفاظ بالمعلومات ونظم الدعم بما يتفق مع احتياجات المؤسســة بأكلمها. وتتكيف نظم المعلومات لدعم التغييرات في مســتويات كثيرة، فمدققو تقنية المعلومات على ســبيل المثال يواجهون كثيراً حالات تكون قد شــهدت تنفيــذ تطبيــق تقنية معلومات منذ ســنوات لدعم احتياجات مختلفــة. وعلى الرغم من إمكانية وجود ضوابط رقابية جيدة للنظام، فإن هذا النظام قد لا يدعم الاحتياجات الحالية للمؤسســة. وتتبنى نظــم الرقابة الداخلية (COSO) رؤية شــاملة لأنواع تلك النظم، كما تشير إلى الحاجة إلى فهم كل من العمليات اليدوية والتقنيات الآلية.

المتابعة:

تعــرض النظرة الهرمية للرقابة الداخلية (COSO) الموضحة بالشــكل التوضيحي (٤-٢) عنصر المتابعة بوصفه المستوى الأعلى والمتطور لعناصر الرقابة الداخلية (COSO). وفي حين أن نظم الرقابة الداخلية ســتعمل بفاعلية مدعومة بشــكل مناسب من الإدارة والإجراءات الرقابيــة وارتباطــات المعلومات والاتصالات؛ لابد من إجراء عمليات لمتابعة تلك الأنشــطة. كانــت المتابعة ولمدة طويلة هي الدور الذي تقوم به تقنية المعلومات وغيرها من المدققين الداخليــين ممن يقومــون بالمراجعات لتقييم مدى الامتثال مع الإجــراءات الموضوعة، لكن ومع ذلك، تتخذ نظم الرقابة الداخلية (COSO) الآن رؤية أوسع للمتابعة أيضاً، كما تعترف بــأن إجراءات الرقابة وغيرها من النظم تتغير بمــرور الوقت. فما ظهر أنه فعالٌ عند بداية تثبيته قد لا يكون فعالاً في المســتقبل نظراً للظــروف المتغيرة والإجراءات الجديدة أو غيرها مــن العوامل. وقد تحتاج المنشــأة إلى وضع مجموعة متنوعة من أنشــطة المتابعة لقياس مــدى فاعلية نظم الرقابة الداخلية لديها من خلال عمليات تقييم منفصلة إلى جانب القيام بأنشطة مستمرة لمراقبة الأداء واتخاذ إجراءات تصحيحية عند الحاجة. فالعديد من إدارات الأعمال الروتينية يمكن تصنيفها على أنها أنشــطة متابعة، وتعطي (COSO) أمثلة على هذا المكون المهم من مكونات الرقابة الداخلية:

الوظائف الاعتيادية لإدارة التشغيل:

تعد المراجعات الاعتيادية التي تجريها الإدارة لعمليات التشــغيل والتقارير المالية أحد أنشطة المتابعة المستمرة الهامة، ولكن ينبغي أن نُولي اهتماماً خاصاً بالاستثناءات المرصودة وانحرافــات الرقابة الداخلية، ومما يعزز الرقابة الداخليــة مراجعةُ التقارير بصفة منتظمة واتخاذ إجراءات تصحيحية لأي استثناءات مرصودة.

اتصالات من أطراف خارجية:

تعتبر وســائل مراقبــة الاتصالات الخارجية مثل رقم هاتف شــكاوى العملاء من الأمور المهمة. كما تحتاج المؤسسة أن تتابع تلك المكالمات عن كثب وتنفذ الإجراءات التصحيحية بناء على هذه المكالمات كلما دعت الحاجة لذلك.

البنية المؤسسية والأنشطة الرقابية:

على الإدارة العليا دائماً القيام بمراجعة تقارير موجزة واتخاذ إجراءات تصحيحية بشــأنها، ويلعب والمســتوى الرقابي الأول في الغالب دوراً أكثر أهمية في عملية المتابعة. كما أن الرقابة المباشرة للأنشــطة الكتابية، على سبيل المثال، ينبغي أن تراجع بشكل روتيني أخطاء المستوى الأدنى وتُصححــه، كما يتعين عليها أن تضمن تحســين أداء الموظفين الكتبة. ويمثل هذا أيضاً أحد المجالات التي يكون من الأهمية بمكان القيام بفصل كاف بين المهام، كما أن تقسيم المهام بين الموظفين يسمح لهم بالقيام بدور متابعة بعضهم لبعض.

الجرد المادي وتسوية الأصول:

إن عمليات الجرد المادي الدوري، ســواء لمخزون المســتودعات أم الأوراق المالية القابلة للتداول أو أصول تقنية المعلومات، تعد من بين أنشطة المتابعة المهمة. فالجرد السنوي في متجر بيع تجزئة مثلاً قد يشــير إلى فقد كبير في البضاعة، وقد يكون أحد الأسباب المحتملة لهذا الفقد هو شبهة سرقة، مما يشير إلى ضرورة وجود نظم رقابة أمنية أفضل.

وليست هذه ســوى أمثلة قليلة من أنشطة المتابعة لنظم الرقابة الداخلية (COSO) التي تُعتبر أشــكالاً من الإجراءات التي ينبغي تنفيذها في العديد من المؤسســات، لكنها في كثير من

الأحيان لا يُنظر إليها على أنها أنشطة متابعة مستمرة. فأي إدارة أو عملية تقوم بمراجعة أنشطة المؤسسة بصفة مستمرة، ثم تقترح إجراءات تصحيحية محتملة يجب النظر إليها باعتبارها نشاط متابعة. وفي حين يشير إطار الرقابة الداخلية (COSO) إلى أهمية أنشطة المتابعة هذه، فإنه يشير أيضاً إلى أنه "قد يكون من المفيد إلقاءُ نظرة جديدة من وقت لآخر على فاعلية نظم الرقابة الداخلية من خلال القيام بتقييمات منفصلة". وتعتمد وتيرة تلك التقييمات أو المراجعات المنفصلة وطبيعتها بشكل كبير على طبيعة المؤسسة وأهمية المخاطر التي يجب مراقبتها.

وحين ترغب الإدارة في بدء إجراء تقييم دوري لنظم الرقابة الداخلية لديها بكاملها، ففي الغالب يجب أن تبدأ بتقييم مجالات رقابية محددة. ويبدأ إجراء هذه المراجعات غالباً عندما تكون هناك عملية استحواذ أو تغيير في قطاع العمل أو في بعض الأنشطة المهمة الأخرى.

وتؤكد (COSO) أيضاً أنه يمكن إجراء هذه التقييمات من قِبل الإدارة التنفيذية المباشرة من خلال إجراء مراجعات تقييم ذاتي. ومع ذلك، يجب على الإدارة المسؤولة في هذا المجال أن تتابع جدولة هذه التقييمات الذاتية وإجراءها بصفة مستمرة. إن هذا النوع من المراجعة المتولدة داخلياً يمكن أن يشير إلى مشاكل رقابية محتملة ويتسبب في أن تقوم إدارة التشغيل بتنفيذ الأنشطة المتعلقة بالإجراءات التصحيحية. ولأن مراجعات التقييم الذاتي تلك لن تكون شاملة مثل التدقيق الداخلي النمطي، فيجب البدء في مراجعات المتابعة إذا تصادف وجود مشاكل كبيرة محتملة، وذلك من خلال القيام بمراجعات تقييم ذاتي محدودة.

عملية تقييم الرقابة الداخلية:

تلخص المواد الإرشادية للرقابة الداخلية (COSO) عملية تقييم مراجعة نظم الرقابة الداخلية. فينبغي لمثل هذا المُقيِّم أولاً أن ينمي لديه فهم تصميم النظام، ثم يقوم باختبار نظم الرقابة الأساسية، ثم يضع استنتاجات بناءً على نتائج الاختبار. كما تشير نظم الرقابة الداخلية (COSO) إلى المقارنة المرجعية، على أنها نهج بديل. وتُعرف المقارنة المرجعية بأنها عملية مقارنة عمليات المؤسسة وإجراءات الرقابة لديها مع مثيلاتها في نظائرها من المؤسسات الأخرى. فيتم إجراء المقارنات مع مؤسسات مماثلة أو مع ما يقابلها من إحصاءات الصناعة المنشورة. ويكون هذا النهج مناسباً لبعض الإجراءات وممتلئاً بالمخاطر

للبعض الآخر. فمثلاً يكون من السهل نسبياً أن تقيس حجم التوظيف ومستوياته ومتوسط التعويضـات لوظيفـة المبيعات مع ما يقابلها من المؤسسـات المماثلـة في الصناعة العامة نفسـها. ومع ذلك، فإن المُقيِّم قد يواجه صعوبات في محاولته مقارنة عوامل أخرى بسبب العديد من الاختلافات الصغيرة التي تجعل جميع المؤسسات فريدة من نوعها.

خطط عمل التقييم:

تقـر نظم الرقابة الداخليـة (COSO) بأن العديد من الإجـراءات الفعالة للغاية تكون غير رسـمية وغـير موثقة. كما أن العديد من نظم الرقابة غـير الموثقة هذه يمكن اختبارها وتقييمها بالأسلوب نفسه المتبع في اختبار النظم الموثقة وتقييمها. وحيث إن وجود مستوى مناسب من التوثيق يجعل أي تقييم لنظم الرقابة الداخلية أكثر كفاءة ويسهل فهم الموظفين لكيفيـة إجراء العمليات، فإن هذا التوثيق لا يكون ضرورياً بصورة مسـتمرة. فأي مراجعة لأنظمة الرقابة المالية الداخلية في المؤسسـة سـيبحث بالتأكيد عن مستوى معين من توثيق النظـم كجزء مـن أعمال المراجعة. فإذا وجدت عملية حالية غير رسـمية وغير موثقة لكن فاعليتهـا محل توافق، فإن فريق المراجعة المعين سـيكون بحاجة إلى إعداد توثيق إجراءات التقييم بهدف شرح كيفية تنفيذ هذه العملية وطبيعة نظم الرقابة الداخلية لديها.

الإبلاغ عن أوجه القصور في الرقابة الداخلية:

سـواء تم تحديـد أوجه قصور الرقابة الداخلية من خـلال العمليات الموجودة في نظام الرقابة الداخلية ذاته أو من خلال أنشـطة المتابعة أو الأحداث الخارجية الأخرى، فإنه يلزم تبليغُها إلى المستويات المختصة في إدارة المؤسسة.

والسؤال الرئيسي الذي يطرحه أي مُقيِّم نظم رقابة داخلية هو تحديد ما ينبغي الإبلاغ عنـه في ضـوء الكم الهائل من التفاصيل التي يمكن أن تواجهـه، ولمن يجب أن توجه هذه التقاريـر. وتنـص نظم الرقابة الداخلية (COSO) عـلى أن، "جميع أوجه القصور في نظم الرقابـة الداخلية التي يمكن أن تؤثر في تحقيق المنشـأة لأهدافها يجب الإبلاغ عنها لأولئك الذيـن يمكنهم اتخـاذ الإجراءات اللازمـة". ورغم أن هذا البيان الصـادر من نظم الرقابة الداخليـة (COSO) يوحـي بداية بأن الأمـرَ معقول، فإن كبار المديريـن من ذوي الخبرة

يدركــون أنــه يكون من الصعب تطبيقه غالباً. إن المؤسســات الحديثــة، بغض النظر عن تنظيمهــا الجيد، ســتكون مدانة بســبب ارتكابها للعديد من الأخطــاء أو الإهمال في نظم الرقابــة الداخلية. وتشــير نظم الرقابة الداخليــة (COSO) إلى أن كل هذه الأمور ينبغي تحديدهــا والإبلاغ عنهــا، حتى ما يبدو أنه أخطاءٌ صغيرةٌ يجــب فحصه لفهم ما إذا كانت ناجمة عن أي قصور في الرقابة بكاملها.

وتســتخدم المواد الإرشــادية المنشــورة من قِبل نظم الرقابة الداخلية (COSO) مثال الموظف الذي اســتولى على بضعــة دولارات من صندوق المصروفــات النثرية، حيث يمكن اعتبار ذلك مســألة بســيطة نظراً لصغر المبلغ المسروق، لكن يكون مــن الضروري اعتباره انهياراً لنظم الرقابة على عدة مستويات.

ففــي حــين أن المبلغ النقدي قد لا يكــون كبيراً، فإن نظم الرقابــة الداخلية (COSO) تحث على أنه يجب فحص هذه المســألة بدلاً من تجاهلها، لأن "هذا التغاضي الواضح عن الاســتخدام الشــخصي لمال المنشأة قد يرسل رســالة غير مقصودة للموظفين". فقبل ظهور قوانين ســاربينز- أوكسلي (SOx)، طبق المدققون الخارجيون بانتظام مفهوم ما كان يسمى "الأهمية النسبية" عند القيام بإجراء المراجعات وقرروا أن بعض الأخطاء والمخالفات كانت صغيرة لدرجة أنها غير جوهرية بالنسبة للاستنتاجات الكلية للمدقق الخارجي.

وفي الســنوات الأولى من مراجعات امتثال قوانين ســاربينز- أوكسلي (SOx) مع معايير التدقيق AS2 الأصلية، كانت رسالة العديد من المدققين الخارجيين تفيد أن الأهمية النسبية لا تؤخذ بعين الاعتبار، فالخطأ هو الخطأ، وقد تســبب هذا النهج في الشعور بالإحباط لدى العديد من المديرين الذيــن تعجبوا من قيام مدققيهم الخارجيين بإثارة قضايا كانوا يرونها قضايا بســيطة، أما الآن ومع قوانين ســاربينز- أوكســلي (SOx) الحالية التي ناقشــناها في الفصل الثاني من هذا الكتاب، فقد وُضعت الأهمية النســبية والمخاطر النســبية في الاعتبار عند تقييم كفاءة نظم الرقابة الداخلية وفاعليتها.

وتختتم الإرشــادات الصادرة عن نظــم الرقابة الداخليــة (COSO) بالنقاش حول من ينبغي توجيه تقرير أوجه قصور نظم الرقابة الداخلية إليه في المؤسسة، وتنص الفقرة الأولى منه على توجيه يفيد في التقييمات:

"إن الآثـار الناتجـة عن أوجه قصـور نظم الرقابـة الداخلية يجب الإبـلاغ عنها ليس للشـخص المسئول عن الإدارة أو النشاط المعني الذي يمكنه بحكم منصبه اتخاذ الإجراءات التصحيحية فحسـب، لكن يجب الإبلاغ عنها في الوقت نفسه لمستوى واحد على الأقل من مستويات الإدارة الأعلى من الشخص المسئول بشكل مباشر. فهذه العملية تمكن ذلك الفرد مـن تقديم الدعـم اللازم أو الإشراف على اتخاذ الإجـراءات التصحيحية وعلى التواصل مع الآخرين في المؤسسـة الذين قد تتأثر أنشطتهم. وحيث إن هذه الآثار قد تتخطى الحدود التنظيمية، فإن الإبلاغ عنها كذلك يجب أن يُنقل إلى مسـتوى أعلى بالدرجة الكافية ويوجه لضمان اتخاذ الإجراءات المناسبة".

كما ينبغي على المؤسسـة أيضاً أن تطور إجراءات الإبلاغ بحيث يتسنى إبلاغ المستويات المناسـبة في المؤسسـة بكل أوجه قصور نظم الرقابة الداخلية التي تتم مواجهتها من خلال مراجعـة العمليات الجارية. ويعتبر إعداد التقارير الإدارية والمتابعة جانباً مهماً للغاية من جوانب نظم الرقابة الداخلية، كما أن للتدقيق الداخلي دوراً رائداً في هذه العملية من خلال مراجعـات تدقيق تقنية المعلومات، ويجب أن نعي أيضاً الحاجة إلى عمليات متابعة أخرى عند مراجعة الرقابة الداخلية وتقييمها.

أبعاد أخرى لإطار الرقابة الداخلية (COSO):

ننسى أحيانـاً أن إطار الرقابة الداخلية (COSO) عبارة عن نموذج ثلاثي الأبعاد كما هو مبين بالشـكل التوضيحي (٤-١)، وبالإضافة إلى البعد الخاص بالواجهة الأمامية الذي يغطي أنشـطة الرقابة، فإن البعد الخاص بالجهة اليمنى يغطي الكيانات أو الأنشـطة، في حين أن الجزء العلوي من مكعب الإطار يغطي جميع عناصر نظم الرقابة الداخلية:

١- فاعلية العمليات وكفاءتها.

٢- موثوقية التقارير المالية.

٣- الامتثال للقوانين واللوائح المعمول بها.

كل مجال من مجالات الرقابة الذي تم مناقشـته حالاً – من بيئة الرقابة إلى المتابعة – يجب أن يؤخذ أيضاً بعين الاعتبار بالنسبة للبعدين الآخرين.

وفيما يتعلق بالبعد الخاص بالجانب الأيمن، يجب تثبيت نظم الرقابة الداخلية وتقييمها عبر جميع الوحدات في المؤسسة. ولا يعني هذا أن نشاطاً رقابياً ما كعملية اعتماد المصروفات مثلاً يجب أن يكون متطابقاً في جميع وحدات المنظمة، سواء في المقر الرئيسي للمؤسسة أم في مكتب مبيعات يقع في منطقة جغرافية نائية. ومع ذلك، يلزم وجود مجموعة متناغمة من عمليات الرقابة عبر المؤسسة بأكملها مع مراعاة الاعتبارات المخصصة للتعامل مع المخاطر النسبية ونطاقات عمليات التشغيل. كما ينبغي أن تكون نظم الرقابة الداخلية متوافقة غير أنه يتم تطبيقها بشكل مناسب في وحدات التشغيل الفردية.

وبالنسبة للبعد الثالث أو العلوي من إطار نظم الرقابة الداخلية (COSO)، فإنه يمثل أهمية أكبر، حيث يفيد بأنه يجب وضع أنشطة الرقابة الداخلية في جميع وحدات تشغيل المؤسسة مع الأخذ في الاعتبار عوامل الرقابة الداخلية الثلاثة: الفاعلية وموثوقية التقارير المالية والامتثال التنظيمي. وعند النظر إلى نظم الرقابة الداخلية من هذا المنظور الثلاثي الأبعاد، ستظهر دائماً بعض الاختلافات، لكنها ستكون تحت إطار رقابة داخلية أساسي ومتسق. فعند استخدام مثال الشركة التابعة في آسيا الوسطى بعيداً عن المقر الرئيسي في الولايات المتحدة، قد تخضع إجراءات اعتماد مصروفات الدولة للقوانين المحلية، كما أن غيرها من العمليات قد تكون مختلفة بعض الشيء نظراً لبعد الاتصالات أو الاختلافات في نظم تقنية المعلومات المحلية. ومع ذلك، يظل من الضروري تنفيذ نظم الرقابة الداخلية تلك على نحو يضمن موثوقية إعداد التقارير المالية إلى جانب إحالة النتائج إلى المقر الرئيسي للمؤسسة.

ومن بين المفاهيم المهمة والمعتبرة للغاية التي تدعم نظم الرقابة الداخلية (COSO) أن جميع الاعتبارات الخاصة بالرقابة الداخلية يتعين النظر إليها طبقاً لمكعب (COSO) ثلاثي الأبعاد، بمعنى أن الرقابة يجب أن تؤخذ في الاعتبار من ناحية توافقها مع المؤسسة بأكملها وعلاقتها بمجالات أهداف الرقابة الثلاثة التي تمت مناقشتها حالاً. ويقدم هذا المفهوم وسيلة فعالة للنظر في نظم الرقابة الداخلية من منظور شمولي. ويظل إطار الرقابة الداخلية (COSO) يمثل معياراً مهماً ومجموعة من المواد الإرشادية لقياس الرقابة الداخلية وتقييمها.

لقـد أصبح إطار الرقابة الداخليـة (COSO) المعيار المعتمد في جميع أنحاء العالم لبناء رقابـة داخليـة فعالة وتطويرها. إنها عمليةٌ مسـتمرةٌ في كلٍ من أبعـاده الثلاثة. فعنصر المتابعـة الموجـود أعلى الجهة الأمامية مـن النموذج لن تكون له قيمة تذكـر ما لم تُفَعل عمليـات الرقابة الداخلية جميعها حتى نصل بها إلى أسـاس بيئـة الرقابة الداخلية. وعلى نحو مماثل، يجب وضع رقابة داخلية فعالة في جميع مستويات وحدات المنظمة، ويلزم أن تراعي نظم الرقابة هذه عناصر الرقابة الداخلية الثلاثة الموجودة أعلى النموذج.

إرشادات متابعة أنظمة الرقابة الداخلية (COSO):

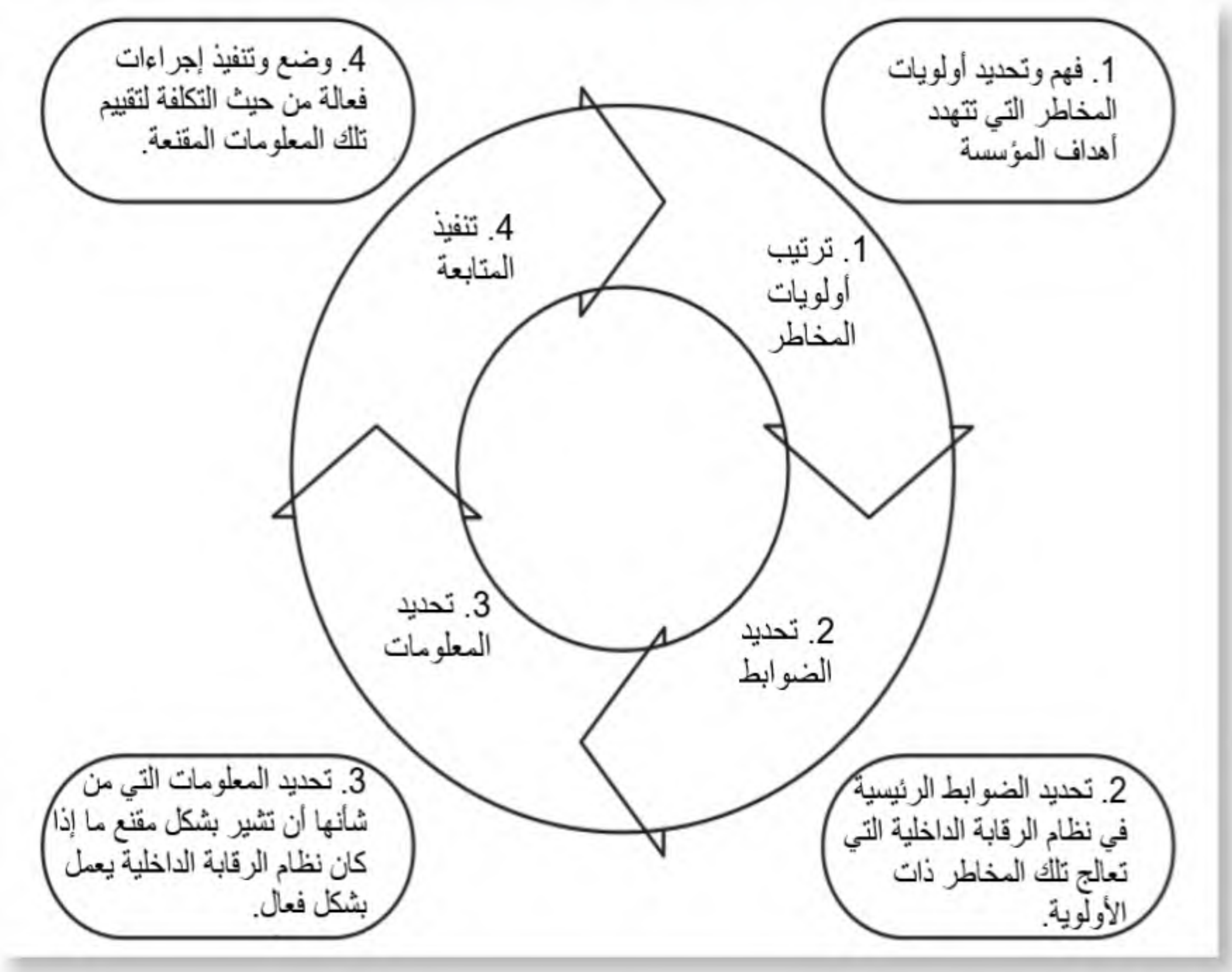
لقد أصبحت المواد الإرشادية واسعة الانتشار عن إطار الرقابة الداخلية (COSO) متاحة من خلال مصادر تتراوح بين معايير تدقيق (AICPA) إلى مختلف مواد (ISACA) بالإضافة إلى موادنـا الإرشـادية الإضافية[٥]، ومع ذلك فـإن العديد من المؤسسـات وليس بالضرورة محـترفي التدقيق قد ترغب في الحصول على إرشـادات أكثر تحديداً عـن كيفية تنفيذ نظم الرقابة الداخلية (COSO) في العمليات التشـغيلية لأعمالها. وقد نشرت COSO مجموعة مواد إرشادية مكونة من ثلاثة مجلدات عن نظم الرقابة الداخلية في عام ٢٠٠٩م[٦].

وتوكـد المجلدات الثلاثة لهذه المجموعة الممتازة بوجه عام أهمية متابعة فاعلية النظم الرقابيـة الموضوعة. وعلى الرغم من وصفنا لإطار الرقابة الداخلية (COSO) كما هو مبين بالشـكل التوضيحي (٤-٢) يُظهر أن المتابعة تعد رأسَ العملية بكاملها، فإن هذه الدراسـة الخاصة بـ COSO تشـير إلى أن بعض المؤسسات لم تسـتغل بالشكل الأمثل نتائج أنشطة متابعتها للخروج باستنتاجات عن فاعلية عمليات الرقابة الداخلية لديها، مما أدى في بعض الأحيان إلى إجراء عمليات غير فعالة تنقصها الكفاءة.

هذه الإرشـادات المتعلقة بأنظمة المتابعة الداخلية توحي بأن المؤسسات تنفذ عمليات المتابعـة الخاصة بالرقابة الداخلية على غرار الطريقة التـي تراقب بها المنظمات الصناعية الفاعلية والكفاءة المسـتمرة لإجراءات التصنيع لديها. وتقترح المواد بأن تقوم المؤسسـات باعتماد عملية متابعة من أربع مراحل كما هو موضح بالشكل التوضيحي (٤-٣).

شكل توضيحي (٤-٣)

عملية متابعة تصميم وتنفيذ الإطار COSO



ينــص هــذا النهج ذو المراحــل الأربع أنه ينبغي عــلى المؤسســة أولاً أن تقوم بتحديد الأولويات وفهم المخاطر التي تتعرض لها أهدافها التنظيمية، ثم تحدد النظم الرقابية التي تعالــج تلك المخاطــر ذات الأولوية. ثم تأتي الخطوة الثالثة وهــي تحديد المعلومات التي من شــأنها أن تشير بشــكل مقنع إلى أن نظام الرقابة الداخلية يعمل بشكل فعال. ويدعو النموذج المقترح إلى القيام بإجراءات مجدية التكلفة لتقييم المعلومات التي تم جمعها من خلال عمليات المتابعة.

تتمة: أهمية الرقابة الداخلية (COSO):

يقـدم هذا الفصل إطار الرقابة الداخلية (COSO) بالغ الأهمية. فمديرو الإدارة العليا يعملون في بيئات مؤسسـية متنوعة، واليوم سـيواجهون في الغالـب متطلبات إطار الرقابة الداخليـة (COSO). وعـلى الرغـم من تقديم هـذا الفصل لمجرد وصف موجـز للرقابة الداخلية (COSO)، فإن المديرين التنفيذيين سيواجهون هذه القضايا عندما يقوم المدققون الخارجيون لديهم بمراجعة نظم الرقابة الداخلية باعتبار ذلك جزءاً من التدقيق المالي، وكذلك عندمـا يقوم مدققوهم الداخليون بمراجعة نظم الرقابـة الداخلية في مجموعة متنوعة من المجالات.

كما يقدم إطار الرقابة الداخلية (COSO) أساسـاً لفهم مدى واسـع من قضايا حوكمة تقنيـة المعلومات التي تناقـش في فصول أخرى لاحقاً. ومن ثم فـإن كبار المديرين يتعين عليهم تكوين معرفة عامة وفهم لإطار الرقابة الداخلية (COSO) أساساً لفهم نظم الرقابة الداخلية للمؤسسة وكذا المسائل المتعلقة بحوكمة تقنية المعلومات.

ملاحظات:

١. بيان معايير التدقيق رقم ١، تقنين معايير وإجراءات التدقيق، AICPA، المعايير المهنية.

٢. تقريـر اللجنة الوطنية حول التقارير الماليـة الاحتيالية (National Commission on Fraudulent Financial Reporting, 1987).

٣. الرقابـة الداخلية - إطار متكامل. هذا المرجع خاص بتقرير الضوابط الداخلية الصادرة عن COSO والذي يمكن طلبه من خلال المعهد الأمريكي للمحاسبين القانونيين AICPA على الموقع www.cpa2biz.com.

٤. تـم وصف معايير الرقابة الداخليـة الخاصة بلجنة المنظمات الراعية COSO في بيانات معايير التدقيق (SASs) أرقام. 103، 105، 106، 107، 109، 110، 112.

٥. انظر "Robert Moeller, Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, and ITIL (Hoboken, NJ: John Wiley & Sons, 2008)".

٦. Guidance on Monitoring Internal Control Systems (COSO, 2009)

الفصل الخامس

إطار كوبت (COBIT) ومعهد حوكمة تقنية المعلومات

يحتــاج المهنيــون المحترفون في المؤسســة وخصوصاً كبــار المديرين أيضاً إلى اســتخدام مجموعــة من المعايــير أو أطر العمل لضبط كل من الممارســات المتعلقــة بحوكمة تقنية المعلومات والإجراءات العامة الخاصة بالرقابة الداخلية. فالالتزام بإطار كهذا سيتيح فرصة اعتماد كبار المديرين وكذلك المهنيين داخل المؤسسة كل في مجال عمله بوصفهم أخصائيين في مجــالات أعمالهم. وقد أصبح إطــار الرقابة الداخلية الخاص بلجنــة المنظمات الراعية (COSO) الذي تم عرضه ومناقشــته في الفصل الرابع من هذا الكتاب من الأدوات الهامة في مجال حوكمة تقنية المعلومات والذي يُســتخدم لتقييم وتحسين عمليات حوكمة تقنية المعلومات المتعلقة بالعديد من النظم والعمليات الخاصة بتقنية المعلومات، ويستخدم أيضاً لتقييم وتحســين قواعد الرقابة المحاسبية الداخلية وفقاً لقانون ساربينز - أوكسلي (SOx)، الذي تطرقنا إليه في الفصل الثاني من هذا الكتاب. وعلى الرغم من ذلك، فقد أعرب بعض كبار المديرين والمهنيين ممن يعملون معهم في مجال تقنية المعلومات على وجه الخصوص عن مخاوفهم من استخدام إطار الرقابة الداخلية (COSO) في ظل عالمنا اليوم المتجه نحو تقنية المعلومات. وقد جاء هذا القلق بســبب عدم تركيز الإرشــادات المنشــورة والخاصة بإطار الرقابة الداخلية (COSO) على أدوات وعمليات تقنية المعلومات بشكل كاف. فعلى ســبيل المثال، تطرقت المواد الإرشــادية الأصلية الخاصة بإطــار الرقابة الداخلية (COSO) والتي تم نشرها عام ١٩٩٢م (انظر الفصل الرابع) في الأساس إلى الضوابط الداخلية الخاصة بتطبيقــات تقنية المعلومات على مســتوى عالٍ، مع أن هناك حاجة لمزيد من الإرشــادات المتعلقة بالرقابة الداخلية لتقنية المعلومات في الوقت الراهن.

إن الإطار الأكثر توجهاً نحو تقييم الرقابة الداخلية لتقنية المعلومات والإرشــادات المتعلقة بهــا يطلق عليه اســم إطار كوبــت Control Objectives for Information and related Technology COBIT (أهــداف ضوابــط المعلومــات والتقنيات ذات الصلــة)، وهو الإطار المعمول به في الواقع قبل ســن قانون ســاربينز أوكسلي (SOx) بوقت طويل، وذلك من خلال

الإصــدار الأول له عام ١٩٩٦. وقــد تم تطوير الإطار كوبت بداية لدعــم المدققين الداخليين والخارجيين الذين يقومون بعمليات مراجعة النظم الحاسوبية والضوابط التقنية (يطلق عليهم غالباً اســم مدققي تقنية المعلومــات IT auditors). لكن كوبت أصبح هذه الأيام هو الأداة المفضلة بالنســبة للعديد من المؤسســات لتحقيق الإمتثال للبنــد ٤٠٤ من قانون SOx الذي يتحــدث عن إجراءات الرقابة الداخلية ودعم حوكمــة تقنية المعلومات المتعلقة بها. فالإطار كوبت يقدم الإرشــادات اللازمة لتقييم وفهم الضوابط الداخلية لتقنية المعلومات المؤسســية ويركز على موارد تقنية المعلومات لدى المؤسسة. لا يمكن اعتبار الإطار كوبت بديلاً عن إطار الرقابــة الداخلية COSO، غير أنه عبارة عن طريقة مختلفة ومفضلة في بعض الأحيان للقيام باختبار ضوابط الرقابة الداخلية في ظل عالمنا اليوم المتمركز حول تقنية المعلومات.

وعلى الرغم من إطلاق "كوبت" بالأســاس ليعمل كدليل توجيهي يســاعد مدققي تقنية المعلومات الداخليين والخارجيــين الذين يقومون بمراجعة الضوابط الداخلية المتعلقة بتقنية المعلومــات، فإنــه تطور هــذه الأيام ليصبــح بمثابة الأداة المســاعدة لتقييــم حوكمة تقنية المعلومــات وجميع الضوابط الداخلية في المؤسســة. فهو يؤكــد الروابط الموجودة بين موارد تقنيــة المعلومات والموارد الأخرى للأعمال ويوفر الإرشــادات الداعمة لهــذه الروابط وذلك لتقديم القيم الكاملة للمؤسســة، كــما يعد هذا الإطار واحداً من الأدوات الهامة لمســاعدة السلطة التنفيذية العليا في المؤسسة على إيجاد ممارسات فعالة لحوكمة تقنية المعلومات.

ســيقدم هذا الفصل نظــرة عامة على المســتوى التنفيذي للإطار كوبــت والعديد من مكوناته الأساســية. وسيســتعرض أيضاً الإصــدار الخامس والأخير لهــذا الإطار حتى وقت نشر هذا الكتاب. كما ســيقوم بتقديم عناصر أخرى للإطار كوبت مثل الإرشادات الخاصة بحوكمــة مجلس الإدارة والإطار الخاص بقيمــة تقنية المعلومات (Val-IT) المرتبط بالإطار كوبت، وهو نهج يســتخدم للتعــرف على القيمة الخاصة بجميع أصــول تقنية المعلومات في المؤسســة بشــكل أفضل. حيث يتناول إطار قيمة تقنية المعلومات Val-IT الافتراضات والتكاليــف والمخاطر والنتائــج المتعلقة بالمحفظة المتوازنة لاســتثمارات الأعمال المدعومة بتقنية المعلومات. كما ســنتحدث أيضاً عن أهمية إطار قيمة تقنية المعلومات Val IT في الفصل الثاني والعشرين من هذا الكتاب. وســيصف لنا هذا الفصل أيضاً العلاقة الموجودة

بين أهداف الإطار كوبت وإطار الرقابة الداخلية COSO والذي تم الحديث عنه في الفصل الرابع من هذا الكتاب.

وعلى الرغم من أن الإطار كوبت ظهر في الأصل أداة إرشادية خاصة بتدقيق تقنية المعلومات، فإنه أصبح في الوقت الحالي أكثر اتساعاً وشمولاً. لذا ينبغي أن يكون لدى المسؤولين التنفيذين اليوم معرفة عالية المستوى برسالة الإطار كوبت وأهدافه، كما ينبغي عليهم أن يكونوا في الموضع الذي يمكنهم من سؤال كلٍّ من إدارة تقنية المعلومات والإدارة العامة لعمليات التشغيل المالية لديهم حول استخدام المؤسسة للإطار كوبت في أنشطة حوكمة تقنية المعلومات. فبالإضافة إلى معرفة وفهم إطار الرقابة الداخلية COSO، فإن فهم الإطار كوبت سوف يساعد المدير الأول على تحقيق مستوى فهم أفضل لدور الرقابة وعمليات الحوكمة والمخاطر الخاصة بتقنية المعلومات في العديد من بيئات المؤسسة.

المقدمة التنفيذية للإطار كوبت:

إن كلمة COBIT تعد غير مألوفة أو غريبة بعض الشيء بالنسبة للعديد من الأشخاص، إلا أن هذا المصطلح أصبح متعارفاً عليه بشكل متزايد من قبل مدققي ومحترفي تقنية المعلومات والعديد من مديري المؤسسات. وعلى الرغم من أن هذا الإطار يُعرف الآن اختصاراً باسم COBIT فإنه في الأصل ولسنوات عديدة كان يكتب CobiT: وفي كلتا الحالتين يشير هذا الاختصار إلى أهداف ضوابط المعلومات والتقنيات ذات الصلة (Control Objectives for Information and related Technology). ونظراً لتركيز هذا الإطار على كل من الضوابط والتقنية، فقد تم استخدام الحروف الكبيرة (C و T) في كتابة الحرف الأول والأخير من الاسم المختصر لهذا الإطار. فالإطار كوبت هو إطار للرقابة الداخلية الخاصة بحوكمة تقنية المعلومات وأداة دعم هامة لتوثيق وفهم المتطلبات الخاصة بالضوابط الداخلية للإطار COSO وقانون ساربنز أوكسلي SOx، وإدراك قيمة أصول تقنية المعلومات في المؤسسة والمخاطر المصاحبه لها. لذا يجب على العديد من أعضاء طاقم التدقيق الداخلي أن يكون لديهم على الأقل معرفة عامة أو عملية بالإطار كوبت. كما ينبغي على كبار المديرين في جميع أنحاء المؤسسة أن يكون لديهم معرفة عامة عن الإطار كوبت وأهميته بوصفة أداة لدعم حوكمة تقنية المعلومات.

قام معهد حوكمة تقنيــة المعلومات IT Governance Institute (ITGI)[1] والمنظمة المهنية الوثيقة الصلة به، وهي جمعية تدقيق وضبط نظم المعلومات (إزاكا) Information Systems Audit and Control Association (ISACA) بإصــدار إطــار العمــل كوبت والمعايــير الخاصة به والتعديل عليها على نحو منتظم. تركز جمعية إزاكا بدرجة كبيرة على عمليــات تدقيق تقنية المعلومات، في حــين ينصب تركيز معهد ITGI على عمليات البحث والحوكمة. كما تقوم جمعية إزاكا أيضاً بإدارة الاختبارات والتصميم المهني لشــهادة مدقق تقنية معلومات معتمــد Certified IT Auditor أو مدقق نظم معلومات (CISA)، هذا إلى جانب إدارتها لـشــهادات أخرى مثل شــهادة مدير نظــم معلومات معتمد Certified Information Systems Manager (CISM)، وتصميــم شــهادة وامتحانــات معتمد في حوكمــة تقنيــة المعلومــات المؤسســية Certified in Governance of Enterprise IT (CGEIT). وتســتهدف شــهادة مدير أمن معلومات معتمد (CISM) مديري أمن تقنية المعلومــات وتعزز من تطوير قدرات المهنيين المحترفين الذين يرغبون في الاعتراف بخبراتهم ومعرفتهم ذات الصلة بحوكمة تقنية المعلومات.

إن العديــد من موظفي إدارة تقنية المعلومــات والموظفين النظاميين في وحدة التدقيق الداخلي هم أيضاً أعضاء في جمعية إزاكا. ولأسباب تتعلق بالتوق إلى الماضي كانت جمعية إزاكا تُعْـرَف في الأصل باســم جمعيــة مدققي نظم معالجــة البيانــات الإلكترونية EDP Auditors Association (EDPAA)، وهــي مجموعة مهنية بدأت في عام ١٩٦٧ من قبل المدققــين الداخليين الذين شــعروا بأن المنظمة المهنية التابعين لهــا والتي عُرفت فيما بعد باسم، معهد المدققين الداخليين Institute of Internal Auditors (IIA)، لم تهتم الاهتمام الــكافي بأهمية نظم تقنية المعلومات والضوابط التقنية باعتبارها جزءاً من أنشــطة الرقابة الداخلية. وقد نسينا أن نذكر أن EDP كانت في يوم من الأيام ترمز إلى Electronic Data Processing أي معالجــة البيانــات الإلكترونية، أما اليوم فإن هــذا المصطلح قد عفا عليه الزمن ولم يعد يُســتخدم في مجال تقنية المعلومات، ومع مرور الوقت قامت هذه المؤسسة المهنية بتوسيع نشاطها وأصبحت جمعية إزاكا.

بــدأت جمعية مدققي نظــم معالجة البيانات الإلكترونيــة EDPAA - والتي كانت في المقام الأول عبارة عن منظمة مهنية حديثة العهد بمجال تدقيق تقنية المعلومات - في تطوير

مواد إرشـادية مهنية خاصـة بتدقيق تقنية المعلومات، وقـد كان ذلك بعد فترة وجيزة من تأسيسـها، وبمجرد أن تطورت جمعيـة EDPAA إلى جمعية ISACA ثم تحولت في الوقت الحـالي إلى معهد ITGI، أصبحت المعايير الأصلية الخاصة بتدقيق تقنية المعلومات الصادرة عنها مجموعة ممتازة من أهداف الرقابة الداخلية والتي تطورت إلى الإطار كوبت، وهو الآن بنسـخته الخامسـة التي أصدرت عام٢٠١١ (٢). وهذا الإصدار الجديد للإطار لم يكن قد تم نشره بشكل رسمي حتى وقت نشرنا لهذا الكتاب، إلا أننا نستند في حديثنا هنا إلى الإصدارات الخاصة بالمسـودة الأخيرة لهذه النسـخة على افتراض أنه سيتم قريباً إطلاقها بشكل رسمي. من الناحية العملية، فإن جميع العمليات المؤسسية ترتبط اليوم بموارد تقنية المعلومات، لذا فإن فهم مجال حوكمة تقنية المعلومات بصورة شاملة أصبح أمراً في غاية الأهمية.

ويتكـون الإطار كوبت مما يطلق عليه اسـم المبادئ الخمسـة five principles، وهي عبارة عن مجالات واسعة ومتداخلة في الحوكمة والضوابط الداخلية، كما هو مبين بالشكل التوضيحي (٥-١). فإن مبادئ الإطار كوبت عبارة عن خمسة مجالات رئيسية تتمحور حول أهمية المبدأ الأساسي لحوكمة تقنية المعلومات، وهذه المبادئ هي:

المبدأ الأول لكوبت: إطار عمل متكامل لتقنية المعلومات: يدعو الإطار كوبت إلى بذل الجهود اللازمة لكي تتماشى عمليات تشـغيل تقنية المعلومات وأنشطتها مع جميع عمليات التشـغيل الأخرى في المؤسسـة. وهذا يشـمل إيجاد الروابط بين عمليات تشغيل الأعمال وخطط تقنية المعلومات في المؤسسة، هذا بالإضافة إلى وضع عمليات لتحديد العلاقات بين الجودة والقيمة والمحافظة عليها والتأكد من صحتها.

المبـدأ الثاني لكوبت: دوافع تحقيـق القيمة لأصحاب المصلحة: يجب أن يكون هناك عمليات متعارف عليها لضمان تقديم وحدة تقنية المعلومات ووحدات التشغيل الأخرى في المؤسسة للقيم والفوائد المرجوة من خلال الدورة الخاصة بتقديمها وباستخدام الإستراتيجية التي تقلص التكاليف مع التأكيد على القيم الذاتية المكتسـبة من أنشطة تقنية المعلومات وغيرها من الأنشطة الخاصة بالمؤسسة.

المبدأ الثالث لكوبت: تركيز الموارد على بيئة أو سـياق الأعمال: مع التركيز على تقنية المعلومات، يجب أن تكون هناك استثمارات مناسبة، وإدارة سليمة، للعناصر الهامة في تقنية

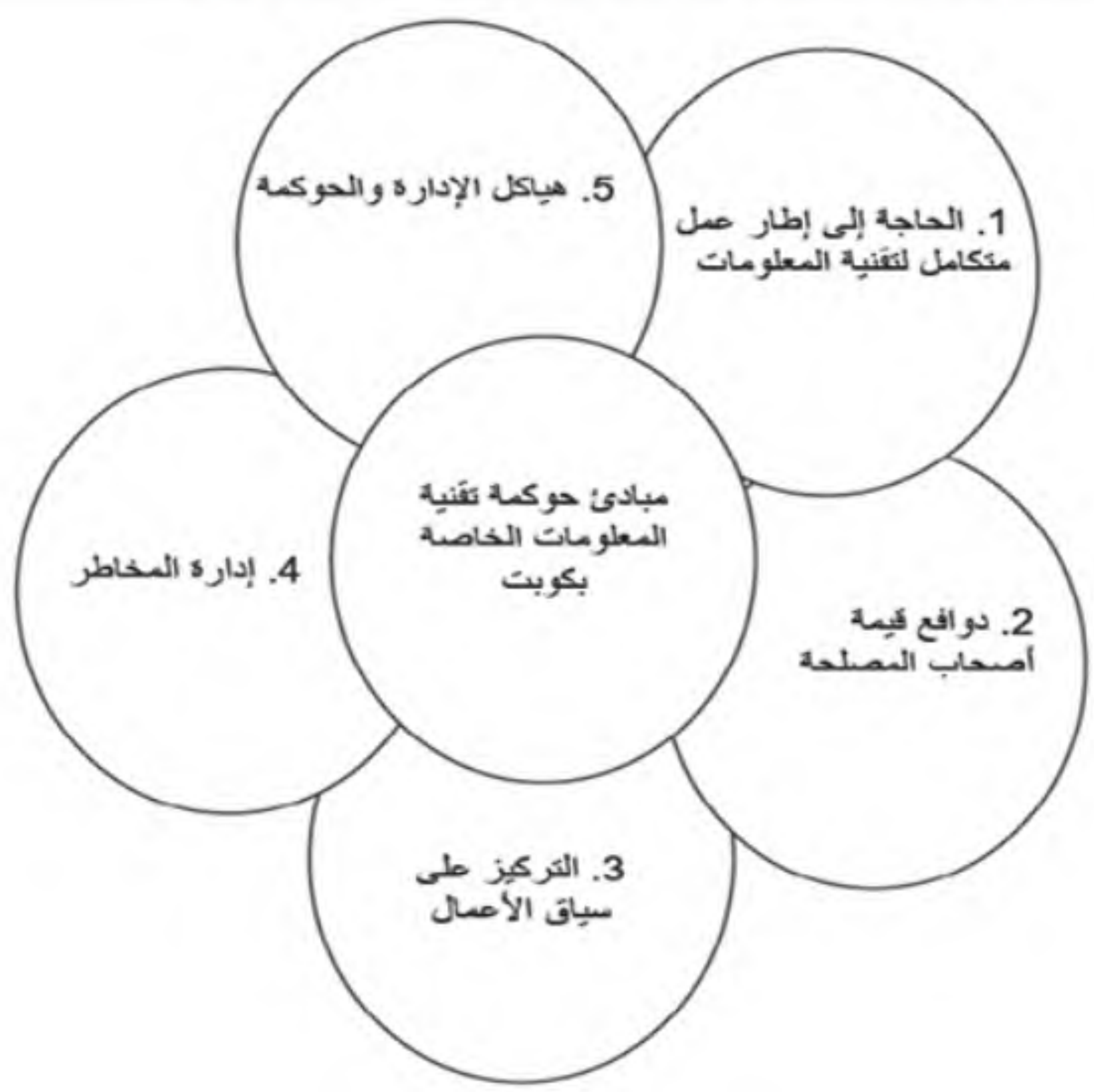
المعلومــات من مــوارد وتطبيقات ومعلومات وبنى تحتية وأفــراد. حيث تعتمد الحوكمة الفعالة لتقنية المعلومات على هذا التحسين في المعرفة والبنية التحتية.

المبــدأ الرابــع لكوبــت: إدارة المخاطر: ينبغــي أن يكون لــدى الإدارة، وعلى جميع المســتويات، فهم واضح لمدى رغبة المؤسســة في المخاطر أو ما يعرف بـ Risk Appetite، ومتطلبــات الامتثال الخاصة بها، وتأثير المخاطر الكبــيرة. فلكل من إدارة تقنية المعلومات وغيرهــا من الإدارات الأخرى مســئولياتها الخاصة والمشــتركة لإدارة المخاطر التي قد تؤثر بشكل فردي أو جماعي على المؤسسة بأكملها.

المبــدأ الخامس لكوبت: قياس الأداء: ينبغي أن تكــون هناك عمليات متعارف عليها ومعمول بها لمتابعة ومراقبة تنفيذ الإســتراتيجية واكتمال المشروع واســتخدام الموارد وأداء العمليــات وتقديم الخدمات. كــما ينبغي أن تقوم آليات حوكمة تقنية المعلومات بترجمة إستراتيجيات التنفيذ إلى إجراءات ومقاييس لتحقيق تلك الأهداف.

شكل توضيحي (٥-١)

مبادئ كوبت الخاصة بحوكمة تقنية المعلومات



هذه هي المبادئ أو مناطق التركيز الخمسة الخاصة بكوبت التي تحدد عناصره وتقدم تعريفاً للعناصر الأساسية لحوكمة تقنية المعلومات. يعتبر الإطار كوبت من الأدوات الفعالة لتوثيــق ضوابط تقنية المعلومات وجميع الضوابط الداخلية الأخرى، وينظر هذا الفصل إلى الإطار كوبت من منظور أشــمل لاستخدامه للمساعدة في عمليات حوكمة تقنية المعلومات الخاصة بالإدارة والمؤسسة ووحدة التدقيق الداخلي.

تقــدم الأجــزاء التالية من هذا الفصل وصفاً شــاملاً للإطار كوبــت، في الصيغة النهائية لمســودة الإصدار الحالي وهو الإصدار الخامس، وعناصره الرئيسية التي تقوم بربط الأعمال مع أهداف تقنية المعلومات من خلال الضوابط الرئيســية ومعايير القياس الفعالة. إضافة إلى أن هذا الفصل سوف يقوم بوصف معايير كوبت مع ما يناظرها في إطار الرقابة الداخلية COSO، والذي تمت مناقشته في الفصل الرابع من هذا الكتاب، وأفضل الممارسات الخاصة بمكتبة البنية التحتية لتقنية المعلومات، التي تم تقديمها في الفصل السادس من هذا الكتاب، والحوكمة الشــاملة لتقنية المعلومات والشركات. كما ســيتم مناقشــة العناصر والمكونات الرئيسية لحوكمة تقنية المعلومات. يعد الإطار كوبت إحدى الآليات الفعالة لتوثيق وفهم الضوابط الداخلية وإدارة عمليات حوكمة تقنية المعلومات على جميع المســتويات. وعلى الرغــم مــن أن كوبت كان في البداية عبــارة عن مجموعة من المواد الإرشــادية الخاصة بـ "تدقيق تقنية المعلومات" فإنه اليوم أصبح أداة أكثر قوة.

إطار العمل كوبت والعوامل المحركة له:

تعد عمليــات تقنية المعلومات والتطبيقات البرمجية والأجهــزة المادية الداعمة لها من المكونات الرئيســية لأي مؤسســة في الوقت الراهن. فســواء كانت هذه المؤسسة من المؤسســات الصغيرة التي تقوم بممارسة عمليات البيع بالتجزئة التي لها احتياجات بســيطة كمتابعة المخزون ودفع رواتب الموظفين، أم كانت من المؤسسات الـكبيرة جداً ضمن تصنيف أفضل خمسين مؤسسة أو "Fortune 50"، فجميعها يحتاج إلى مجموعة كبــيرة من عمليات تقنية المعلومات المترابطة والمعقدة أحياناً والتي ترتبط ارتباطاً وثيقاً بعمليات تشــغيل الأعــمال المتعلقة بها. بمعنى أنه، ينبغــي أن يعمل كل من عمليات الأعــمال وموارد تقنية المعلومات الداعمة لها في المؤسســة ضمــن علاقة وثيقة لتبادل

المعلومــات. لا يمكن لتقنيــة المعلومات - وبالتأكيد لا ينبغي - أن تكشــف لعمليات تشــغيل الأعمال عن الأنواع الخاصة بعمليات ونظم تقنية المعلومات التي ينبغي عليها تنفيذهــا، ولكنها تقوم بتوفــير المعلومات التي تؤثر في قرارات تلــك الأعمال. في الأيام الأولى لظهور نظم الحاســبات، شــعر المديرون في بعض الأحيــان، بأنهم يملكون العديد من الإجابات والحلول المطورة للنظم المتعلقة بأعمالهم، إلا أنها أحياناً كانت تأتي بنتائج عكســية تمامــاً. ومع ذلك، فإن هــذه العلاقة قد تغيرت منذ فــترة طويلة؛ فبوجه عام ينبغي أن تكون هناك علاقة وثيقة لتبادل المعلومات والمتطلبات المشــتركة بين عمليات تشــغيل تقنية المعلومات وعمليات تشــغيل الأعمال. وينبغي على مدير المؤسسة فهم الاحتياجات والمتطلبات اللازمة لتبادل المعلومات بين الطرفين. فتقنية المعلومات لديها مســئوليات تجاة المجالات الأخرى المرتبطة بالعمليــة التي يتم تدقيقها من قبل أو من خلال إرشــادات التدقيق المعتمدة، التي يتم قياســها من خلال سلســلة من القياسات والأنشــطة الخاصة بمؤشر الأداء، التي يتم تفعيلها من خلال أهداف النشــاط. كل ذلك أصبح جزءاً لا يتجزأ من كوبت الذي يعد إطاراً لحوكمة وضبط تقنية المعلومات ويحدد أهداف أفضل الممارســات والحوكمة والرقابة الداخلية لــكل عملية من عمليات تقنية المعلومات والأعمال.

فبالإضافــة إلى إطــار الرقابة الداخليــة COSO ومتطلبات الضوابــط الداخلية لقانون ســاربنز أوكســلي SOx، يقدم هذا الفصل الإصدار الخامس والجديد لكوبت. وقد يتساءل أحد المسؤولين التنفيذيين للمؤسسة قائلاً: "أعتقد أنني أفهم بعض القواعد الرئيسية لقانون ســاربنز أوكســلي SOx، وأن مؤسســتي تقوم باســتخدام إطار الرقابة الداخلية COSO؛ فلماذا يجب علي الاهتمام بهذا الشيء المســمى كوبــت، واعتماده كإطار آخر؟" إن إجابتنا عــن هذا التســاؤل هــي أن كوبت يوفر نهجاً بديــلاً بل وأحياناً مفضــلاً لتعريف ووصف العمليات التي تركز عــلى حوكمة تقنية المعلومات بصورة أكثر من الإطار التقليدي للرقابة الداخليــة COSO. في هذه الأيام تعتبر المعلومــات والعمليات الداعمة لتقنية المعلومات هي بالفعل الأصول الأكثر أهمية وقيمة بالنسبة لجميع المؤسسات. وتقع على عاتق الإدارة مســؤولية كبيرة وهي الحفاظ على الأصول الداعمة لتقنية المعلومات، متضمناً ذلك النظم الآلية. ويحتاج المسؤول التنفيذي في المؤسسة هذه الأيام إلى فهم هذه العمليات المرتبطة

بالمعلومات والضوابط الداعمة لها. وتهتم هذه التركيبة بفاعلية وكفاءة جميع الموارد والعمليات والمتطلبات الشاملة لأعمال تقنية المعلومات الخاصة بها.

يقر الإطار كوبت بأن المعلومات يجب أن تكون أحد الموارد الرئيسية لجميع المؤسسات، حيث إن هناك اعتمادية هائلة على التقنية طيلة دورة حياة المعلومات بالكامل. حيث تنتشر تقنية المعلومات والتقنيات المرتبطة بها في المؤسسات، وهي بحاجة إلى أن تُحْكم وتدار بطريقة شمولية، مع أخذ كامل المسؤولية المتعلقة بجميع مجالات الأعمال ومهام تقنية المعلومات بصورة تامة (من النهاية إلى النهاية). فمن خلال التنفيذ الفعال لإرشادات الإطار كوبت. يجب على المؤسسة أن تحقق المزيد من:

- إيجاد القيمة من خلال تقنية المعلومات المؤسسية.
- رضا مستخدمي الأعمال عن الأعمال والخدمات التي تقدمها تقنية المعلومات.
- الالتزام بالقوانين واللوائح والسياسات ذات العلاقة.

وكما ذكرنا، فقد استمر تطوير وتحسين الإطار كوبت على مر السنين. وقد اعتمدنا في تعليقاتنا في هذا الفصل في المقام الأول على الإصدار الخامس الجديد الذي كان في مسودتة النهائية أثناء القيام بتأليف هذا الكتاب. كما سنقوم أيضاً بتضمين بعض المراجع التي تشير إلى الإصدار السابق للإطار كوبت - الإصدار ٤,١ - والمعترف به على نحو جيد. إن النسخة الجديدة كوبت ٥,٠ (COBIT 5.0) تعد تحسيناً كبيراً للنسخة السابقة، كما أنها توفر دعماً وإرشادات ممتازة لتحسين عمليات حوكمة تقنية المعلومات، ورغم أنه قد تكون هناك بعض التعديلات النهائية عندما يتم إطلاق الإصدار الخامس بشكل رسمي، فإن العديد من الأوصاف التي استخدمناها للإطار كوبت توحي بأنه سيتم إطلاق الإصدار الجديد والنهائي قريباً. واستناداً إلى مبادئ كوبت الخاصة بحوكمة تقنية المعلومات والموضحة في الشكل التوضيحي (٥-١)، فإن الأقسام التالية سوف تقدم مستوى رفيعاً ونظرة تنفيذية عامة لكوبت، ولماذا يعد هذا الإطار من الأدوات الهامة في حوكمة تقنية المعلومات.

المبدأ الأول لكوبت: إنشاء إطار متكامل لبنية تقنية معلومات:

تصف البنية المعمارية كيف نقوم ببناء المقر الرئيسي الخاص بمكتبنا أو النمط المستخدم في بنائه، إلا أنها هذه الأيام تستخدم غالباً للإشارة أيضاً إلى الاختيارات التقنية لبنية تقنية المعلومات في المؤسسة. فعلى سبيل المثال، عندما تحولت إدارت تقنية المعلومات من نظم الحاسبات المركزية القديمة التي كانت موجودة منذ عدة سنوات إلى الشبكات التي تحتوي على خوادم أصغر حجماً، فقد أعلنت إدارة تقنية المعلومات في المؤسسة بأنها اعتمدت وطبقت البنية التي تدعى "العميل - الخادم". وتستخدم إدارات تقنية المعلومات مصطلح بنية أو معمارية النظم لتشير إلى الشكل العام للأجهزة المادية أو البرمجيات الخاصة بموارد تقنية المعلومات لديها. يمتلك كوبت أيضاً البنية أو المعمارية الخاصة به؛ ومع ذلك، فإن النسخة المنشورة الحالية لبنية كوبت (كوبت ٥,٠) قد تخيف غير المتخصصين في تقنية المعلومات بسبب تعقيدية الرسم التخطيطي للإطار في مسودته الحالية. الشكل التوضيحي (٥-٢) عبارة عن رسم تخطيطي مبسط لمكونات البنية المعمارية الخاصة بالإصدار الخامس لكوبت (كوبت ٥,٠).

وبالرجوع إلى معمارية كوبت والعودة إلى خطوات بدايته، نجد أن المبدأ المهم هنا هو أن عمليات كوبت والعمليات الأخرى التي تخص حوكمة تقنية المعلومات تكون مدفوعة باحتياجات أصحاب المصلحة بدءاً من الإدارة العليا التي تأمل في تحسين عمليات حوكمة تقنية المعلومات، والتي ربما تكون من خلال الإدارة المحلية لتقنية المعلومات التي ترغب هي الأخرى في تحسين عمليات محددة في تطبيقاتها. ويكون أصحاب المصالح عادة عبارة عن مجموعات كبيرة ومختلفة يتشاركون ويختلفون أحياناً في بعض الاهتمامات والأمور التي تتعلق بعمليات حوكمة تقنية المعلومات في المؤسسة. ويتم تقديم هذه الاهتمامات أو الاحتياجات إلى العمليات المعتمدة لكوبت، مع التركيز على أهداف حوكمة وقيمة تقنية المعلومات. أضف إلى ذلك أن كوبت لا يمكن الاعتماد عليه بمفرده ، إذ لا بد من تنسيق هذه الاحتياجات مع المعايير والأطر والعمليات الأخرى الموجودة في المؤسسة.

وكما هو موضح في الشـكل التوضيحي (٥-٢)، فإن هذه الاحتياجات تتحقق من خلال العنـاصر التـي يطلق عليها كوبت اسـم "عنـاصر التمكين"، وهي عبارة عن سلسـلة من العمليـات المنفصلـة والمترابطة والتي سـنتطرق إليها لاحقاً في هـذا الفصل. والغرض من عناصر التمكين هذه هو - كما يشـير إليه الاسـم - تنفيذ وتطبيق العمليات الخاصة بنظم حوكمة وإدارة تقنية المعلومات المؤسسـية. وقد تم تعريف عناصر التمكين بشكل موسع على أنها عمليات أو آليات محددة، أو أي شيء يمكن أن يساعد في تحقيق أهداف الحوكمة المؤسسية. ويشمل ذلك موارد كالمعلومات والأفراد. يحدد إطار كوبت ٥,٠ سبع فئات من عناصر التمكين هي:

١- العمليات

٢- المبادئ والسياسات.

٣- الهياكل التنظيمية.

٤- المهارات والكفاءات.

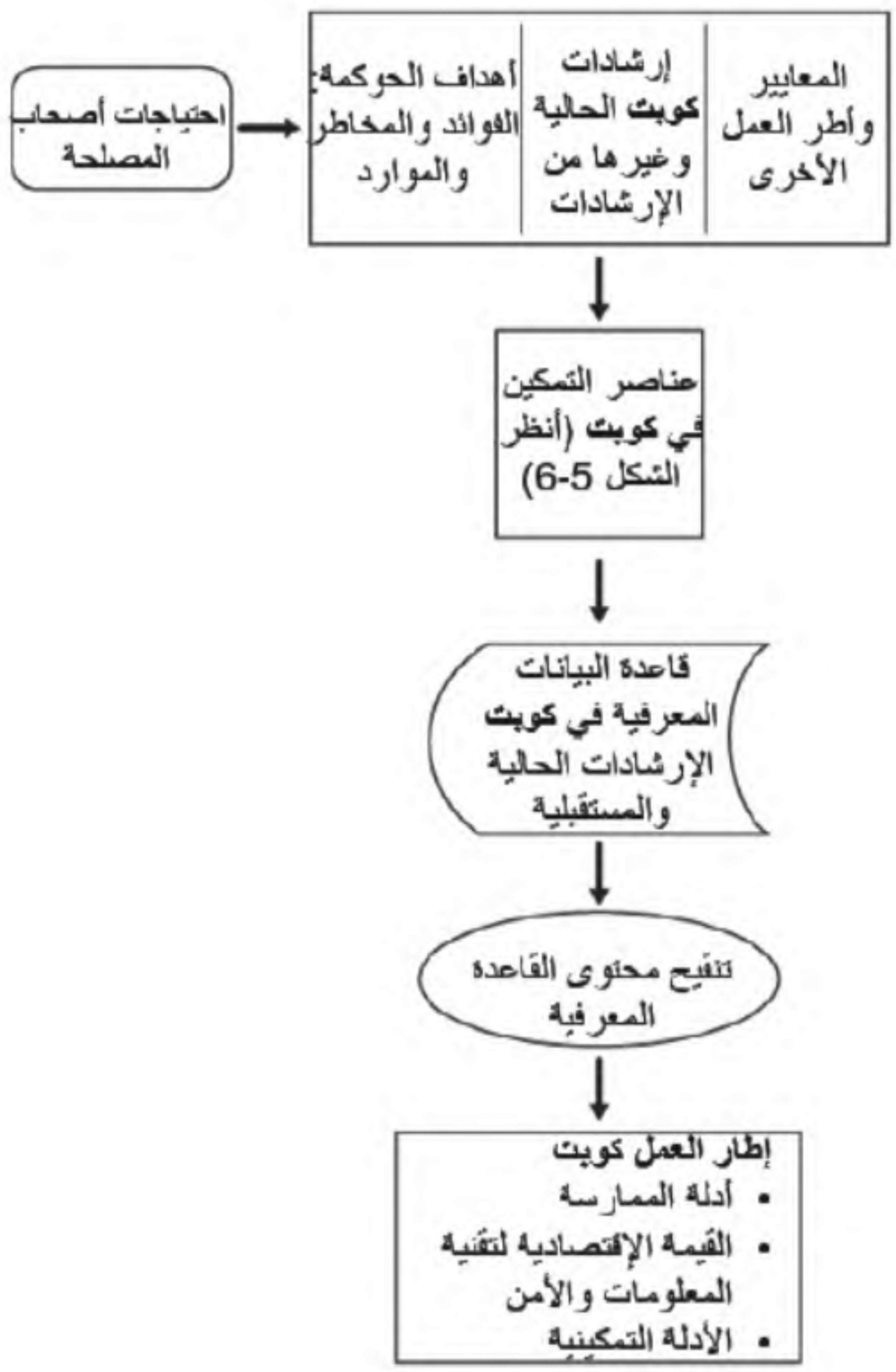
٥- الثقافة والسلوك.

٦- القدرات الخدمية.

٧- المعلومات.

شكل توضيحي (٥-٢)

البنية العامة المبسطة لكوبت ٥



تتفاعل هـذه العناصر التمكينية معاً بطريقة منتظمة، وهـذا يعني أن نظام الحوكمة والإدارة لا يمكـن أن ينجـح إلا إذا تم تنـاول جميع عناصر التمكـين والتعامل معها وفهم التفاعلات الرئيسـية الخاصة بها. وسـنقوم لاحقاً في هذا الفصل بمناقشـة عناصر التمكين الخاصة بكوبت.

بعد ذلك سـتقوم عناصر التمكين المسـتخدمة بتوفـير الدعم اللازم لقاعـدة البيانات المعرفيـة لكوبـت، والتي تتضمن المواد الإرشـادية الحاليـة والهياكل الخاصة بالأنشـطة المسـتقبلية. وسيسـهم كل ذلك في تقديم الدعم المناسـب لتطبيق جميع عمليات الإطار

كوبت والمدعومة أيضا بواسـطة مجموعة من الإرشـادات المتعلقة بالمنتجات والإرشادات المرجعية. إن فكرة البنية المعمارية لكوبت أو الفائدة المرجوة منها هي دعم أهداف إطار العمـل من خلال تزويد جميع أصحاب المصلحة بالإرشـادات الأكثر اكتمالاً وحداثة، وهي تتعلـق بحوكمـة وإدارة تقنية المعلومات المؤسسـية. ولتحقيق هذه الفائـدة، فإن البنية المعمارية لكوبت تضم مجموعة واسـعة من المكونات الآلية والمكونات المتعلقة بالبيانات، مثل المواد الإرشادية التي تحدثنا عنها في فصول أخرى. وسيتم لاحقاً في هذا الفصل مناقشة الغرض من هذه العناصر التمكينية ووظيفتها بمزيد من التفاصيل.

كوبت هـو مجموعة من المـواد التوجيهية التي تدعم العناصر الرئيسـية للإرشـادات الخاصة بـحوكمة تقنية المعلومات، والتي تتضمن العديد من المفاهيم والموضوعات المتعلقة بالتقنيات الخاصة بحوكمة وإدارة المؤسسـة. لقد قامت المؤسسـات بمختلف أحجامها وفي جميع أنحاء العالم بتطبيق كوبت بنسخته السابقة ٤,١. أما الإصدار الجديد لكوبت (كوبت ٥,٠) فإنه يقدم تحسـينات للحـد من المخاطر المتعلقة بتقنية المعلومـات وزيادة الثقة في المعلومات التي تقدمها تقنية المعلومات، لتمكن من تطوير سياسة واضحة وممارسات جيدة لإدارة تقنية المعلومات، وزيادة القيمة المكتسبة من تقنية المعلومات وإدارة الامتثال.

المبدأ الثاني لكوبت: دوافع تحقيق قيمة لأصحاب المصلحة:

يتحقـق تركيز عمـل كوبت من خلال تحديـد جميع أصحاب المصلحـة واحتياجاتهم وتحديد الكيفية التي يرتبطون بها مع قرارات وأنشطة الحوكمة والإدارة. ولنا أن نتصور أن أصحاب المصلحة المستفيدين من عملية تقنية المعلومات وعمليات تشغيلها منقسمون إلى مجموعتين: داخليين وخارجيين. وإن عمليات تشـغيل وعمليات تقنية المعلومات منتشرة بشكل كبير، وإن مجموعة أصحاب المصالح الداخليين الذين تم تحديدهم من خلال كوبت تشمل أعضاء مجلس الإدارة، الرئيس التنفيذي CEO، المدير المالي (CFO)، المدير التنفيذي للمعلومـات (CIO) ومديـري الأعمال التنفيذيـين، وأصحاب عمليـات الأعمال، ومديري الأعـمال، ومديـري المخاطر، ومديري الأمـن ومديري الخدمات، ومديـري الموارد البشرية (HR) والمدققين الداخليين ومسـتخدمي تقنية المعلومات، ومديري عمليات تشغيل تقنية المعلومات، وغيرهم الكثير. وسيكون لكل من هؤلاء توقعات ومواقف مختلفة حول القضايا

الخاصة بحوكمة تقنية المعلومات. والشـــكل التوضيحـــي (٥-٣) يلخص بعض الاحتياجات النمطية لأصحاب المصلحة الداخليين وفقاً للإطار كوبت.

شكل توضيحي (٥-٣)

الاحتياجات القياسية لأصحاب المصلحة الداخليين طبقاً لكوبت

- في ضوء أمن تقنية المعلومات، والمخاوف المتعلقة بالخصوصية، وغيرها من القضايا، هل قمنا بتناول جميع المخاطر ذات الصلة بتقنية المعلومات؟
- هل نقوم بتنفيذ عمليات تشغيل فعالة ومرنة لتقنية المعلومات؟
- كيف يمكننا ضبط تكاليف تقنية المعلومات بشكل أفضل؟
- كيف يمكننا استخدام موارد تقنية المعلومات بالأسلوب الأكثر فاعلية وكفاءة؟
- ما خياراتنا الأكثر فاعلية وكفاءة لتوريد معدات تقنية المعلومات؟
- هل لديّ ما يكفي من الأفراد لتشغيل وإدارة تقنية المعلومات، وكيف يمكنني تطوير والحفاظ على مهاراتهم وإدارة أدائهم؟
- كيف نحصل على ضمانات بشأن نتائج وأداء عمليات تقنية المعلومات؟
- هل المعلومات التي نقوم بمعالجتها مؤمنة بشكل جيد؟
- كيف لنا أن نقوم بتحسين مرونة الأعمال من خلال بيئة تقنية معلومات أكثر مرونة؟
- هل جميع مستويات الإدارة وعمليات التشغيل على بصيرة بما تقوم به تقنية المعلومات؟
- هل تفشل مشروعات تقنية المعلومات كثيراً في تحقيق ما وعدت به؟
- إلى أي مدى تكون تقنية المعلومات هامة لاستمرارية المؤسسة؟
- كيف لنا أن نعرف أن تقنية المعلومات وعمليات التشغيل ذات الصلة الخاصة بشركاء الأعمال لدينا آمنة ويمكن الاعتماد عليها؟
- كيف لي أن أعرف أن المؤسسة متوافقة مع القوانين واللوائح المعمول بها؟
- كيف لنا أن نعرف إذا كانت المؤسسة تحافظ على نظام فعال للرقابة الداخلية؟

كـما تضـم مجموعة أصحاب المصالـح الخارجيين كلاً مــن شركاء العمل والموردين والمســاهمين والجهــات التنظيمية أو التشريعية (الحكومة) والمســتخدمين الخارجيــين والعملاء ومنظمات المعايير القياســية والمدققين الخارجيين والاستشــاريين والعديد من الجهات الأخــرى المعنية بعمليات وموارد تقنية المعلومات. وتشمل احتياجات أصحاب المصلحة الخارجيين أسئلة مثل:

- كيف يمكنني معرفة ما إذا كانت عمليات شريكي في العمل آمنة ويمكن الاعتماد عليها؟
- كيف يمكنني معرفة ما إذا كانت هذه المؤسسة ووحداتها التنظيمية متوافقة مع القواعد واللوائح المعمول بها؟
- كيف لي أن أعرف ما إذا كانت المؤسسة تحافظ على نظام فعال للرقابة الداخلية؟

هناك عدة دوافع يمكن أن تؤثر في احتياجات أصحاب المصلحة منها التغييرات التي تطرأ على الإســتراتيجية، والأعــمال، والبيئة التنظيمية، والتطورات التقنية. وتتجســد احتياجات أصحاب المصلحة هذه في سلسلة من التوقعات أو المخاوف أو المتطلبات المحتملة؛ كل هذه القضايا ترتبــط بواحد أو أكثر من أهداف الحوكمة الثلاثــة العامة الخاصة بكوبت، وهي: تحقيق الفوائد وموازنة المخاطر وتحسين التكلفة.

إن الغرض من وجود المؤسســات هو إيجاد قيمة لأصحاب المصلحة لديها. ومن ثم فإن هــدف الحوكمة لأية مؤسســة - تجارية أو غير تجارية - هو إيجــاد القيمة وتحقيق فوائد بتكلفة مثالية للموارد مع الحد من المخاطر. فالمؤسسات لديها العديد من أصحاب المصلحة الداخليين والخارجيين. و"إيجاد القيمة" يعني أشياء مختلفة - وأحياناً متعارضة - لكل منهم. فالحوكمــة عبارة عن التفاوض واتخاذ القرارات بشــأن تقديم الحلول والتوفيق بين المصالح المختلفــة لأصحاب المصلحة فيما يخص تحقيق هذه القيمــة. ومن ثم فإنه يجب أن يقوم نظام حوكمة تقنية المعلومات بالنظر إلى جميع أصحاب المصلحة عند القيام بعمل تقييمات واتخاذ قرارات بشأن الفوائد والموارد والمخاطر. إن السؤال الذي يمكن، بل وينبغي أن يطرح لكل عنصر من هذه العناصر الخاصة بإيجاد القيمة هو: لمن ستكون الفوائد والمخاطر؟ وما الموارد المطلوبة لتقنية المعلومات؟

المبدأ الثالث لكوبت: التركيز على سياق الأعمال:

كـما ذكرنا في تعليقاتنا السـابقة، بدأ كوبت في الأسـاس أداة لتدقيق تقنية المعلومات، فهو عبارة عن مجموعة محسنة من العمليات المُوصَى بها لمراجعة وتقييم إجراءات الرقابة الداخليـة الخاصة بتقنية المعلومات. كيف تغيرت الأشـياء على مر السـنين؟ ففي الوقت الراهن، يقوم الإطار كوبت بتوفير مجموعة قوية من المواد الإرشادية التي تساعد المؤسسة على تحسين عمليات حوكمة تقنية المعلومات، فالمبدأ الأساسي لكوبت هو التركيز على سياق الأعمال.

يؤكد المبدأ الرئيسي الثالث لكوبت أن الغرض من وجود المؤسسـات هو خلق أو إيجاد قيمة لأصحاب المصلحة. وهناك ثلاثة أهداف لقيمة الحوكمة المعرفة من قِبَل كوبت هي:

١- تحقيق الفوائد.

٢- تحسين المخاطر.

٣- تحسين الموارد.

يعمل كوبت على ربط كل هدف من هذه الأهداف الثلاثة بالأهداف المالية والأهداف المتعلقـة بخدمـة العملاء والأهـداف الداخلية في المؤسسـة. يقوم كوبـت أيضاً بتحديد مجموعة من الأهداف المالية للمؤسسـة، والتي تم تقسـيمها إلى عدة فئات من الأهداف المؤسسـية أي الأهداف المالية، وأهداف العملاء، والأهـداف الداخلية، والأهداف الخاصة بالتعلم والنمو. الشكل التوضيحي (٥-٤) يعرض ملخصاً لأهداف الحوكمة في كوبت مقابل الأهداف المالية للمؤسسة من حيث كونها علاقة رئيسة أو ثانوية مع أهداف قيمة الحوكمة المعرفة من قبل كوبت.

شكل توضيحي ٥-٤

ملخص أهداف الحوكمة في كوبت مقابل الأهداف المؤسسية

أهداف المؤسسة		أهداف الحوكمة		
		تحقيق الفوائد	تحسين المخاطر	تحسين الموارد
المالية	١. القيمة المتحققة لأصحاب المصلحة من استثمارات الأعمال	ر		
	٢. محفظة من المنتجات والخدمات التنافسية	ر		ث
	٣. إدارة مخاطر الأعمال (وقاية الأصول)		ر	ث
	٤. التوافق مع القوانين والقواعد التنظيمية الخارجية		ر	
	٥. الشفافية المالية	ر	ث	ث
العميل	٦. ثقافة خدمية موجهة نحو العميل	ر		ث
	٧. استمرارية خدمات الأعمال وإتاحتها		ر	
	٨. مرونة الاستجابة للتغيرات في بيئة العمل	ر		ث
	٩. اتخاذ القرار الإستراتيجي استناداً إلى المعلومات	ر	ر	ر
	١٠. تحسين تكاليف تقديم الخدمات	ر		
الداخلية	١١. تحسين الأداء الوظيفي لعمليات الأعمال	ر		ر
	١٢. تحسين تكاليف عمليات الأعمال	ر	ر	ر
	١٣. إدارة برامج التغيير في بيئة العمل	ر		ث
	١٤. الإنتاجية التشغيلية وإنتاجية طاقم العمل		ر	ر
	١٥. التوافق مع السياسات الداخلية	ث	ث	
النمو	١٦. أفراد ذوو مهارة ومتحمسون	ر		ر
	١٧. ثقافة الابتكار في المنتجات والأعمال	ر		

أما الشكل التوضيحي (٥-٥) فما هو إلا وثيقة أكثرُ تفصيلاً للغرض من الأهداف المالية. حيث تُظْهِر المواد الأصلية المنشــورة لكوبــت علاقات أكثر تفصيلاً لكل هدف من الأهداف الثلاثة للحوكمة، كل واحد منها مقابل الأهداف المؤسسية.

هذه المقابلة التفصيلية تســاعد على وصف المبدأ الثالث لكوبت الذي يركز على سياق الأعمال، ويتعين على هذه العلاقات أن تساعد الإدارة على مختلف مستوياتها وكذلك أعضاء طاقــم العمل على فهم العلاقات والروابط الموجودة بين عمليات تقنية المعلومات وكل من أنشطة الأعمال الداخلية والخارجية على نحو أفضل.

شكل توضيحي (٥-٥)

مقابلة الأهداف المالية التفصيلية للحوكمة في كوبت مع الأهداف المؤسسية

أهداف تقنية المعلومات المؤسسية		الأهداف المالية للمؤسسة				
		التوافق مع القوانين والقواعد التنظيمية الخارجية	إدارة مخاطر الأعمال (حماية الأصول)	محفظة من المنتجات والخدمات التنافسية	القيمة المتحققة لأصحاب المصلحة من استثمارات الأعمال	الشفافية المالية
		١	٢	٣	٤	٥
المالية	١. القيمة المتحققة لأصحاب المصلحة من استثمارات الأعمال		ث	ر	ر	
	٢. محفظة من المنتجات والخدمات التنافسية	ر	ث		ث	
	٣. إدارة مخاطر الأعمال (وقاية الأصول)		ث	ث	ر	
	٤. التوافق مع القوانين والقواعد التنظيمية الخارجية	ث	ر			
	٥. الشفافية المالية			ر	ر	

العميل	٦. ثقافة خدمية موجهة نحو العميل		ث		ث	
	٧. استمرارية خدمة الأعمال وإتاحتها	ث	ث	ر	ر	ر
	٨. مرونة الاستجابة للتغيرات في بيئة العمل		ث	ث	ث	
	٩. اتخاذ القرار الإستراتيجي استناداً إلى المعلومات		ث	ر	ث	
	١٠. تحسين تكاليف تقديم الخدمات	ر	ر			
الداخلية	١١. تحسين الأداء الوظيفي لعمليات الأعمال			ر	ر	
	١٢. تحسين تكاليف عمليات الأعمال		ث	ث	ث	
	١٣. إدارة برامج التغيير في بيئة العمل		ث	ث	ر	
	١٤. الإنتاجية التشغيلية وإنتاجية طاقم العمل	ث	ث	ر	ث	
	١٥. التوافق مع السياسات الداخلية	ث	ث			
النمو	١٦. أفراد ذوو مهارة ومتحمسون		ر	ث	ث	
	١٧. ثقافة الابتكار في المنتجات والأعمال			ر	ث	

المبدأ الرابع لكوبت: عناصر تمكين إدارة المخاطر والحوكمة:

كـما هو واضح في الوصف الموجـز الذي قدمناه للبنية المعماريـة لكوبت، فإن عناصر التمكـين تعد من العناصر الرئيسـية في عملية الحوكمة الخاصـة بكوبت. فهي عبارة عن العناصر الملموسة وغير الملموسة التي تجعل شيئاً ما يعمل، وفي هذه الحالة فإن هذا الشيء هو حوكمة وإدارة تقنية المعلومات في المؤسسة. تُظْهِر البنية العامة المبسطة "الكوبت ٥,٠" في الشـكل التوضيحي (٥-٢) وظيفة تسمى عناصر التمكين في وسط العملية الشاملة، التي لابد أن تتبناها المؤسسة لتتمكن من حوكمة تقنية المعلومات.

وقد حدد كوبت سـبعة أصناف أو أنواع مختلفة مـن عناصر التمكين. كما هو موضح بصورة منفصلة في الشـكل التوضيحي (٥-٦). فلكي تحقق المؤسسة أهدافها الرئيسية فإنه يتوجـب عليها أن تدرك دائماً بأنها تقوم بـإدارة مجموعة مترابطة من عناصر التمكين التي تمتلكها. ويعرض الشـكل الخاص بالبنية العامة سـبع فئات من عناصر التمكين المترابطة. فعناصر التمكين التي حددها كوبت هي:

١- **العمليات:** هي تلك المجموعات المنظمة من الممارسـات والأنشطة التي تحقق أهدافاً معينة وتُنتِج مجموعة من المخرجات لدعم الأهداف الشاملة المتعلقة بتقنية المعلومات.

٢- **الثقافـة والاخلاقيـات والسـلوك:** إن الثقافة القوية للمؤسسـة إلى جانب التركيز على أخلاقيات العمل وسلوكيات أصحاب المصلحة الداعمة لتلك القيم يتم التقليل من شأنها غالباً إلا أنها من عوامل التمكين الهامة لنجاح أنشطة الحوكمة والإدارة.

٣- **الهياكل التنظيمية:** تعتبر الأنشـطة والسياسـات والترتيبات التنظيمية بمثابة الوسـائل الرئيسية لصنع القرار في المنظمة.

٤- **المعلومـات:** تكـون مهمـة نظراً لأنهـا العنصر المنتـشر في جميع أنحـاء أي منظمة، فالمعلومات ضرورية للحفاظ على تشـغيل المنظمة وحوكمتها بشـكل جيد، ولكن على المستوى التشغيلي فإن المعلومات تكون غالباً هي المنتج الرئيسي للمؤسسة نفسها.

٥- **المبادئ والسياسات:** تعد عناصر التمكين هذه وسيلة لترجمة السلوكيات المرغوب فيها إلى إرشادات عملية للإدارة اليومية.

٦- **المهـارات والكفاءات:** وترتبط هذه السـمات بالعناصر البشريـة وهي ضرورية لإتمام جميع النشاطات بنجاح واتخاذ القرارات الصحيحة.

٧- **القدرات الخدمية:** يشتمل هذا العنصر التمكيني على البنية التحتية والتقنية والتطبيقات التي توفر للمؤسسة معالجة المعلومات وتقديم الخدمات.

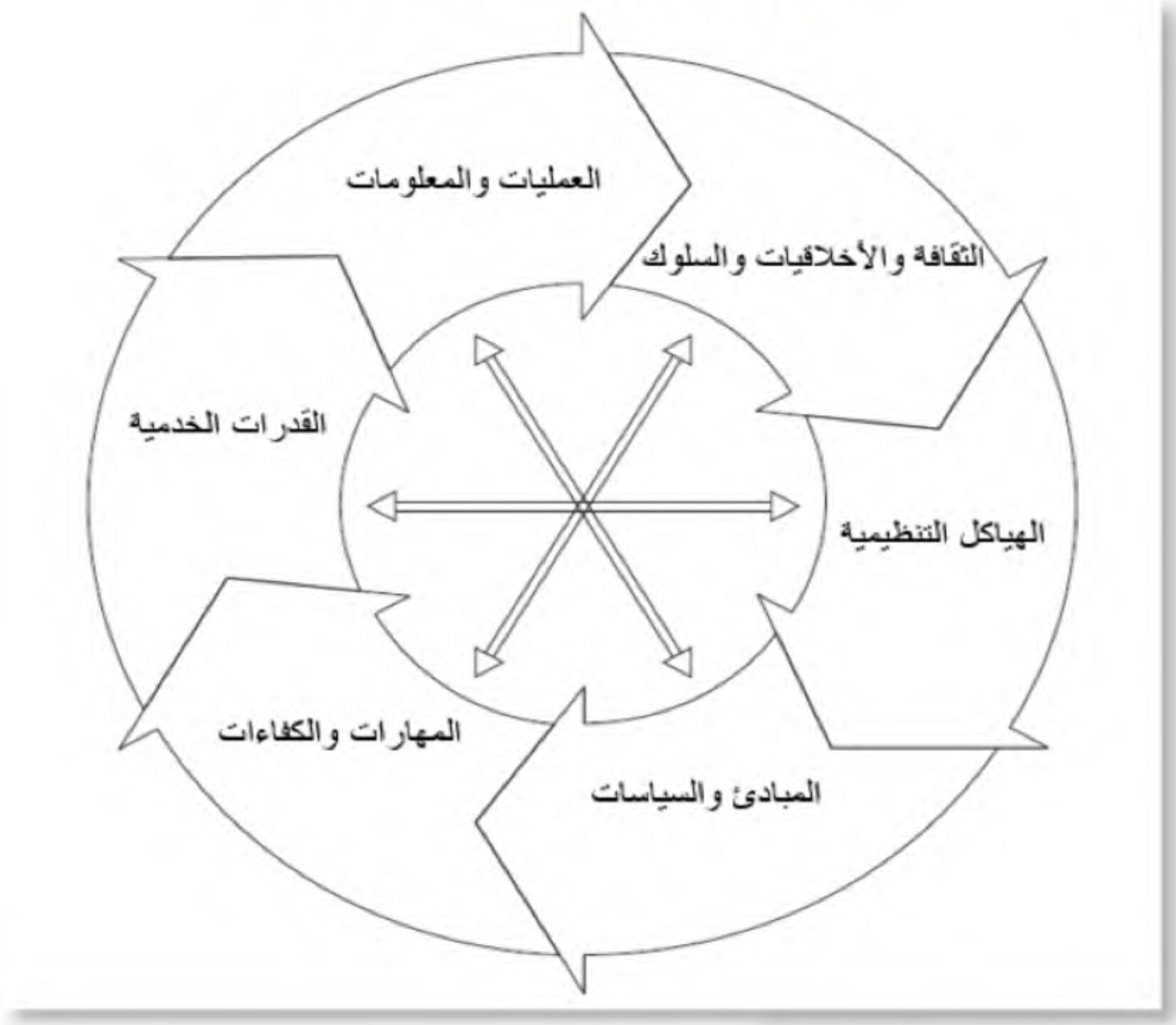
لا يمكن تواجد أي عنصر من عناصر التمكين السـبع تلك بشكل منفرد فجميعها بحاجة إلى مدخـلات من عناصر تمكين أخرى والتي حددها كوبت لكي تكون فعالة بشـكل كامل. فمثلاً نجد أن العمليـات تحتاج إلى عنصر تمكين المعلومات، والهياكل التنظيمية تحتاج إلى عنصر تمكين الناس، والناس بحاجة إلى المهارات والسلوك. فعناصر التمكين توفر المخرجات لصالـح عناصر التمكين الأخرى (على سـبيل المثـال، العمليات توفـر المعلومات والمهارات والسـلوك). ولـكل من هذه العناصر التمكينية السـبعة التي عرفهـا كوبت والموضحة في الشكل التوضيحي (٥-٦) خمسة مكونات نوعية هي:

١- **أصحاب المصلحة لعنصر التمكين:** على الرغم من أننا قد تحدثنا عن أهمية أصحاب المصالح باعتبارها عوامل محركة لعملية كوبت بشـكل كامـل، فإن لكل عنصر من عناصر التمكين السبعة أصحاب المصلحة الداخليين والخارجيين الخاصين به(*) .

(*) الأطراف التي تلعب دوراً نشطاً و/ أو لديهم اهتمام بهذا العنصر (المترجم).

شكل توضيحي ٦-٥

أصناف أو أنواع عناصر التمكين في كويت



فللعمليــات أصحاب مصالح داخليين وخارجيــين، ولكل منهم أدواره الخاصة، لذا يجب توثيق أصحاب المصلحة ومستويات مسئولياتهم بطريقة تعبر عن سمات العملية.

٢- الأهــداف والمقاييس المعياريــة(*): ينبغي تحديد أهداف عنــصر التمكين على أنها بيــان يصف النتيجة المأمولة من العملية. فقد تكون هذه النتيجة عبارة عن منتج صناعي Artifacts، أو تغييراً كبيراً على حالة العملية، أو تحســناً كبيراً في إمكانيات عمليات أخرى. وهــي تمثل جزءاً من أهــداف العملية التي تدعــم الأهداف المتعلقة بتقنيــة المعلومات، والتي بدورها تدعم أهداف المؤسســة. في كل مســتوى، يجب أن تقوم المقاييس المعيارية

(*) مؤشرات (المترجم).

بتعريف وقياس إلى أي مدى تم تحقيق هذه الأهداف. ويمكن تعريف المقاييس المعيارية على أنها كيانات قابلة للقياس الكمي وينبغي أن تكون محددة Specific، وقابلة للقياس Measurable، وقابلة للتنفيذ Actionable، وذات صلة Relevant، وضمن إطار زمني (محددة بوقت) Timely.

ويمكن تصنيف الأهداف بطرق مختلفة تتراوح بين الأهداف الاقتصادية، التي تعتبر أكثر توجهاً نحو تحقيق الكفاءة Efficiency، إلى أن تصل إلى أهداف الجودة، التي تعتبر أكثر توجهاً نحو تحقيق الفاعلية Effectiveness.

وبالمثل فإن هناك نوعين من مقاييس العملية: مقاييس الأداء التي لها طابع تنبؤي وهي تشير إلى مدى تنفيذ العملية للأنشطة المحددة، ومقاييس النتائج التي تشير إلى حجم أو مدى تحقيق العملية لأهدافها والغاية من وجودها.

٣. **دورة حياة عناصر التمكين:** لا بد من دعم كل من عناصر التمكين تلك بالخطط اللازمة لتأسيسه ومن ثم تأتي مراحل البناء والاستحواذ والإنشاء والتنفيذ له. وبعد استخدامها أو تشغيلها، فإن عناصر التمكين يجب أن تُراقب وتُقيّم بشكل دوري مع تحديث الهدف أو التخلص منها عند الضرورة.

٤. **الممارسات الجيدة:** لا بد من وضع وتحديد الممارسات الداخلية والخارجية باستخدام أدوات مثل الإطار كوبت. فهناك مكونات داخلية وخارجية للممارسات الجيدة لعناصر التمكين، وكلاهما يشتمل على ممارسات جيدة في المهارات البشرية، متضمناً ذلك المتطلبات المهارية الموضوعية لكل دور من الأدوار التي يلعبها أصحاب المصالح المختلفين. ويمكن وصف ذلك من خلال التوصيفات الوظيفية المحددة لمستويات المهارات المختلفة باختلاف فئات أو أنواع المهارات. فأنواع أو فئات المهارات تعتمد على الأنشطة المرتبطة بتقنية المعلومات كإدارة شبكة الاتصالات أو تحليل الأعمال.

٥. **سمات عناصر التمكين:** لكل عنصر من عناصر التمكين هذه بعض السمات الفريدة التي تميزه عن غيره من العناصر التمكينية الأخرى الموجودة في المؤسسة.

"عنــصر التمكين" هو مصطلح أو مفهوم لم يكن شـائعاً في عمليات تشـغيل وعمليات الأعمال قبل عدة سـنوات. وقد اشتهر هذا المصطلح بداية من خلال الأوراق العلمية التي تتحــدث عن قضايا تقنية المعلومات. وعلينا أن نتذكر أن عنصر التمكين هو أداة أو عملية توفر القدرات والكفاءات القابلة للقياس والتي من شـأنها أن تحسن عمليات الأعمال، بدلاً من أن تقوم فقط بأتمتها. وهي عبارة عن قدرات وقوى وموارد تسـهم في نجاح الكيان أو النشاط أو المشروع. إنها مفاهيم تستحق أن تضاف إلى قاموس مصطلحات أعمال المرء.

المبدأ الخامس لكوبت: هياكل قياس أداء الحوكمة والإدارة:

يركــز المبدأ الرئيسي والأخير لكوبــت على أهمية المفاهيم المختلفة إلا أنها مترابطة لكل من الإدارة والحوكمة في المؤسســة الموجهة نحو تقنيــة المعلومات. فقد ميز الإطار كوبت ٥,٠ بشكل واضح وجلي بين الحوكمة والإدارة. فكلاهما يتضمن أنواعاً مختلفة من الأنشطة ويتطلب هياكل تنظيمية مختلفة ويخدم أغراضاً مختلفة. فهذا التمييز يعد أساسياً بالنسبة لنظرة كوبت للحوكمة والادارة.

إننا ننسى كثيراً أن الحوكمة governance، ذلك المصطلح الشـائع في عالم الأعمال اليوم، مشـتقة من الفعل اليوناني الذي يعنى "التوجيه" "to steer". حيث يشـير نظام الحوكمة إلى كل الوسـائل والآليـات التـي تمكن العديد مـن أصحاب المصلحة في المؤسســة من أن يكون لهم كلمة مؤثرة في تقييم الظروف والخيارات؛ تحديد الاتجاه؛ متابعة التوافق والأداء والتقدم المحرز مقابل الخطط الموضوعة لتلبية أهداف مؤسسـية محددة. وكل هذا يشير إلى مجموعة كبيرة من الأنشطة التوجيهية. وتشتمل الوسائل والآليات هنا على أطر العمل والمبادئ والسياســات والرعاية والهياكل وآليات صنع القرار إلى جانب الأدوار والمسئوليات والعمليات والممارســات اللازمــة لتحديد الاتجاه ومتابعة الامتثال والأداء الذي يتســق مع الأهداف الشاملة. هذا هو التعريف الكبير والشامل نوعاً ما لحوكمة تقنية المعلومات، إلا أن الفصول التالية سوف تناقش القضايا الأخرى التي تدعم هذا التعريف. وعلينا أن نتذكر دائماً أنه في معظم المؤسسات، تكون الحوكمة مسؤولية مجلس الإدارة وتحت قيادة الرئيس التنفيذي CEO ورئيس مجلس الإدارة.

يتم غالباً تمييز الإدارة عن الحوكمة، فالإدارة تستلزم الاستخدام العادل للموارد والناس والعمليات والممارسات وغير ذلك لتحقيق الغاية المرجوة. فهي الوسيلة أو الأداة التي بها يحقق كيان (أو هيئة) الحوكمة نتيجة أو هدفاً. فالإدارة مسئولة عن التنفيذ ضمن الاتجاه الذي تم تحديده أو وضعه من قبل هيئة أو وحدة التوجية. فالإدارة تتعلق بالتخطيط والبناء والتنظيم ومراقبة الأنشطة التشغيلية لتتماشى مع الاتجاه الموضوع من قبل هيئة الحوكمة.

تؤكد الإرشادات الخاصة بكوبت أن الحوكمة والإدارة هما نوعان مختلفان من الأنشطة، ولكل منهما مسؤوليات مختلفة. ومع ذلك، وبالنظر إلى دور الحوكمة - في التقييم والتوجيه والمراقبة - فإن هناك مجموعة من التفاعلات المتبادلة المطلوبة بين الحوكمة والإدارة للحصول على نظام حوكمة ذي كفاءة وفاعلية. إذ يتم ربط هذه التفاعلات، باستخدام البنية المعمارية لعناصر التمكين، بعمليات محددة لمراجعة الضوابط الداخلية، التي تعد نقطة القوة الحقيقية لإطار العمل كوبت.

مطابقة عمليات كوبت مع أهداف تقنية المعلومات من خلال الجمع بينهما:

يحدد إطار العمل كوبت ومواده الداعمة المنشورة مجموعة رفيعة المستوى من العمليات التي تحدد اتجاه أهداف أعمال المؤسسة وموارد تقنية المعلومات. وهي التي صُممت خصيصاً لتناسب إلى حد ما جميع أحجام المؤسسات وأنواعها، وقد تم تصنيف هذه العمليات إلى مجموعتين: الأولى باعتبارها عمليات لحوكمة تقنية المعلومات المؤسسية، والثانية هي مجموعة منفصلة من العمليات التي تقوم بتقديم الإرشادات الخاصة بإدارة تقنية المعلومات المؤسسية. تحتوي كل مجموعة من هاتين المجموعتين على سلسلة من الإجراءات أو العمليات الأكثر تفصيلاً. فبالنسبة لإدارة تقنية المعلومات في المؤسسة، هناك مجموعات من العمليات أو الإجراءات للقيام بالتالي:

- التوفيق والتخطيط والتنظيم.
- البناء والاستحواذ والتنفيذ.
- تقديم الخدمة والصيانة والدعم.
- التقييم والتوجيه والمتابعة.

كل مجموعــة من هذه المجموعات تتضمن بعد ذلــك عمليات أكثر تحديداً في كوبت. فبالنسبة لمجموعة البناء Build والاستحواذ Acquire والتنفيذ Implement فإن إرشادات كوبت تكون منظمة على شــكل فئات لتحقيق أهداف الرقابة الداخلية باســتخدام أسماء الترميز التالية المعرفة من قبل كوبت:

BAI1- إدارة البرامج والمشروعات

BAI2 - تحديد المتطلبات

BAI3 - تعريف وبناء الحلول

BAI4 - إدارة الإتاحة والسعة

BAI5 - تمكين التغيير التنظيمي

BAI6 - إدارة التغييرات

BAI7 - قبول وانتقال التغييرات

BAI8 - إدارة المعرفة

وقد تم تعريف مجموعة مشــابهة من فئات أهداف الرقابة الخاصة بالعملية لكل فئة مــن فئات العملية المذكورة. إن الغرض من عمليات الرقابة التفصيلية، وإن كانت محددة إلى حد ما، هو المســاعدة في دراســة الحالة المؤسســية Business Case لتنفيذ وتحســين حوكمة وإدارة تقنية المعلومات. هدفها هو التعرف على كل نقطة من نقاط الألم أو النقاط الحرجة الأساســية والأحداث المحفزة، وذلك من خلال الهدف العام لخلق البيئة المناســبة لعمليات تشغيل تقنية المعلومات وتطبيقاتها.

لقــد قام كوبت بتعريف مجموعة مكونة من ١٧ هدفاً مرتبطاً بتقنية المعلومات يمكن مناظرتها مع كل عملية من هذه العمليات. وتنقســم هذه الأهداف أيضاً إلى فئات أخرى معنونــة بـ "الشركــة" و"العميل و"داخليــاً" و"التعلم والنمو". وقد تتغــير هذه العناوين عندما يتحول كوبت من مســودة النســخة النهائية الحالية، ففئة مثل "الشركة" لا تعني أن الإرشادات تنطبق فقط على الشركات العامة، بل على المؤسسات بأكلمها.

الشكل التوضيحي (٥-٧) يوضح المقابلة أو المناظرة بين أهداف كوبت المتعلقة بتقنية المعلومات والعوامل الخاصة بعمليتين من عمليات كوبت هما: (التقييم والتوجية والمتابعة) evaluate, direct, and monitor (EDM) و(تقديم الخدمة والصيانة والدعم) deliver, service, and support (DSS). فهذه المناظرة توضح كيف يتم دعم كل هدف من الأهداف المتعلقة بتقنية المعلومات من قبل إحدى عمليات كوبت. كما هو مبين بالشكل التوضيحي (٥-٧) والذي تم التعبير عنه باستخدم مقياس معين حيث إن:

• ر ترمز إلى علاقة رئيسية بين الهدف الخاص بتقنية المعلومات وعملية كوبت المرتبطة به، عندما تكون هناك علاقة هامة حيث تكون عملية كوبت المصممة داعماً رئيسياً لتحقيق هدف تقنية المعلومات.

• ث ترمز إلى ثانوي ذلك عندما لاتزال هناك علاقة أقل أهمية وتكون عملية كوبت داعماً ثانوياً لهدف تقنية المعلومات.

• فراغ عندما لا توجد في هذه الحالة علاقة قوية.

على سبيل المثال تمتلك عملية كوبت التي يرمز لها بالرمز DSS7 والخاصة بـ "إدارة الأمن" علاقة قوية أو رئيسية مع هدف تقنية المعلومات المدعو أو المسمى "الامتثال ودعم القوانين واللوائح التنظيمية" الخاصة بالمؤسسة. العملية DSS7 نفسها لها أيضاً علاقة ثانوية مع العديد من الأهداف الأخرى لتقنية المعلومات مثل الهدف رقم سبعة (٧) والخاص بتقديم خدمات تقنية المعلومات وفقاً لمتطلبات الاعمال.

تؤكد إرشادات كوبت أن الحوكمة والإدارة هما نوعان مختلفان من الأنشطة، لكل منهما مسؤولياته المختلفة. ومع ذلك، ونظراً للدور التوجيهي الذي تلعبه الحوكمة - للتقييم والتوجيه والمتابعة - فإن هناك مجموعة من التفاعلات التبادلية الضرورية بين الحوكمة والإدارة للوصول إلى نظام حوكمة ذي كفاءة وفاعلية. ويتم بعد ذلك الربط بين هذه التفاعلات وعمليات محددة في كوبت خاصة بمراجعة الرقابة الداخلية، وذلك باستخدام البنية المعمارية لعناصر التمكين، وهو ما يعد القوة الحقيقة للإطار.

بالنســبة للعديــد من كبار المديرين. قــد يبدو إطار العمل كوبت أكــثر تفصيلا، وأنه يحتــوي على مجموعة من الغايات والأهداف المعقــدة بعض الشيء. ومن الممكن تحقيق الفائــدة القصوى من اســتخدام كوبت فقــط إذا تم تبنيه على نحو فعــال وتكييفه ليلائم البيئة الفريدة لكل مؤسسة. فكل نهج تطبيقي سيكون أيضا بحاجة إلى أن يُعَالِج تحديات محددة، بما في ذلك إدارة تغيرات الثقافة والسلوك. لقد لمس هذا الفصل فقط الهيكل العام لكوبت وإصداره الحالي (الاصدار الخامس).

شكل توضيحي (٥-٧)

مثال المقابلة بين أهدف الإطار كوبت وأهداف تقنية المعلومات

			الأهداف المتعلقة بتقنية المعلومات																
			المواءمة بين استراتيجية تقنية المعلومات واستراتيجية المؤسسة	توافق تقنية المعلومات ودعمها للتوافق مع قوانين ولوائح المؤسسة	إدارة مخاطر العمل ذات الصلة بتقنية المعلومات	تحقيق فوائد من الاستثمارات ومحفظة الخدمات ذات الصلة بتقنية المعلومات	الشفافية في تكاليف تقنية المعلومات وفوائدها ومهامها	تقديم خدمات تقنية المعلومات بما يتوافق مع متطلبات العمل	والمعلومات والحلول التقنية	الاستخدام المناسب للتطبيقات	مرونة تقنية المعلومات	أمن المعلومات والبنية التحتية التي تعالجها والتطبيقات	تحسين أصول تقنية المعلومات ومواردها وقدراتها	تمكين ودعم دمج التطبيقات والتقنيات في عمليات الأعمال	الاستفادة المثلى من موارد تقنية المعلومات وقدراتها	إتاحة معلومات موثوقة ومفيدة	توافق تقنية المعلومات مع السياسات الداخلية	أفراد أكفاء متحفزون للعمل بتقنية المعلومات	معرفة وخبرة ومبادرات تدعم الابتكار في العمل
		عمليات الإطار كوبت	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠	١١	١٢	١٣	١٤	١٥	١٦	١٧
			الشركة						العميل		الداخلية							التعلم والنمو	
تقييم وتوجيه ومتابعة	EDM1	قم بوضع وصيانة إطار عمل الحوكمة	ر	ث	ر	ث	ث	ث	ر		ث	ث	ث	ث	ث	ث	ث	ث	ث
	EDM2	تأكد من تحسين القيمة	ر		ث		ر	ر	ر	ث			ث	ث	ث	ث		ث	ر
	EDM3	تأكد من تحسين المخاطر	ث	ث	ث	ر		ر	ث	ث		ر			ث	ث	ر	ث	ث
	EDM4	تأكد من تحسين الموارد	ث		ث		ث	ث	ث	ث	ر		ر		ث			ر	ث
	EDM5	تأكد من شفافية أصحاب المصلحة	ث	ث	ر			ر	ر						ث	ث	ث		ث
تقديم الخدمة وصيانة ودعم	DSS1	قم بإدارة عمليات التشغيل		ث		ر	ث		ث	ث	ث	ث	ر			ث	ث		
	DSS2	قم بإدارة العمليات		ث		ر	ث		ث	ث	ر			ث	ث		ث	ث	
	DSS3	قم بإدارة التهيئة		ث		ث				ث	ث	ث	ث			ث			
	DSS4	قم بإدارة طلبات وحوادث الخدمة				ر			ث	ث		ث						ث	
	DSS5	قم بإدارة المشاكل		ث		ر	ث		ث	ث	ث		ر	ر	ر	ر	ث		ث
	DSS6	قم بإدارة الاستمرارية	ث	ث		ر	ث		ر	ث	ث	ث	ث			ر	ث	ث	ث
	DSS7	قم بإدارة الامن	ث	ر		ر			ث	ث		ر			ث	ث			
	DSS8	قم بإدارة ضوابط عمليات الاعمال		ث		ر			ر	ث		ث		ث		ث	ث	ث	ث

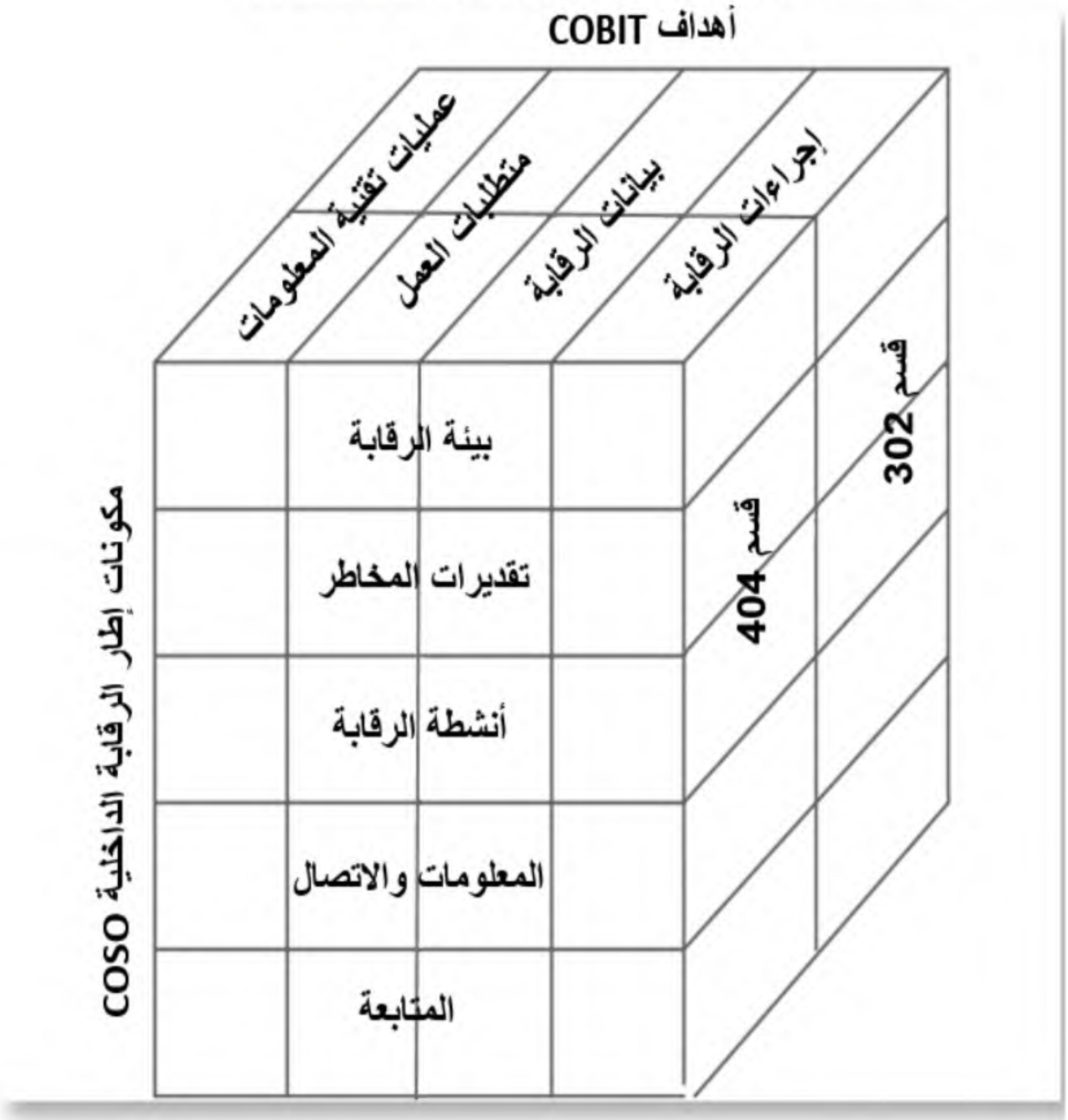
استخدام كوبت في بيئة قانون ساربينز أوكسلي (SOx):

عندما تم تفعيل قانون ساربنز أوكسلي SOx للمرة الأولى في الولايات المتحدة، كان هناك القليل من الإرشادات حول كيفية تطبيق وإدارة البند ٤٠٤ من هذا القانون والخاصة بمراجعات الرقابة الداخلية. وقد أشار مجلس الإشراف المحاسبي على الشركات المساهمة Public Company Accounting Oversight Board (PCAOB) ، الذي تقدم عرضه في الفصل الثاني من هذا الكتاب، إلى أنه كانت لديه النية لوضع بعض المعايير المحددة، إلا أنه قد تعمد في البداية ترك المؤسسات والمدققين الخارجيين دون توجيه. ومع التشديد المكثف على أنظمة الرقابة الداخلية الرفيعة المستوى لتقنية المعلومات، قامت العديد من المؤسسات بتبني الإطار باعتباره إطاراً خاصاً بالرقابة الداخلية على أنه أحد الخيارات التي تساعد في تحقيق الامتثال لقانون ساربنز أوكسلي SOx.

قام البند ٤٠٤ من قانون ساربنز أوكسلي SOx الخاص بمتطلبات تقييم الرقابة الداخلية بتسليط الضوء على النهج القائم على المخاطر لتقييم الضوابط الداخلية مع التأكيد على إطار الرقابة الداخلية COSO، الذي تم الحديث عنه في الفصل الرابع من هذا الكتاب. يعد كوبت بمثابة إطار عمل بديل وقوي لتقييم الضوابط الداخلية ولاسيما في البيئات التي تركز بشكل مكثف على عمليات وموارد تقنية المعلومات. ويمكن وصف كلٍّ من الرقابة الداخلية الخاصة بلجنة المنظمات الراعية (COSO) وكوبت على أنها أطر عمل متعددة الأبعاد لوصف بيئات الرقابة الداخلية الخاصة بكلٍ منهما. فكل منهما يشبه الآخر ولكن مع وجود اختلافات طفيفة في التصنيفات والمصطلحات. الشكل التوضيحي (٥-٨) يبين المناظرة أو المقابلة بين الإطار كوبت ونموذج الرقابة الداخلية (COSO).

شكل توضيحي (٥-٨)

العلاقة بين مكونات COSO وأهداف COBIT



يمكــن اســتخدام أهداف كوبت، بدءاً مــن التخطيط والبدء في تنفيذ المشــاريع وصولاً إلى المتابعــة والتقييــم لفهم وتقييم الضوابط الداخلية من خلال المكونات الخمســة لإطار الرقابة الداخلية COSO. وســواء تم اســتخدام إطار الرقابة الداخلية COSO بشكل عام أم تم اســتخدام كوبت، فإن تحليل هذين الإطارين اللذين ينطلق من خلالهما سلسلة من العمليــات تبدأ مــن التخطيط إلى إجراء تقييمات المخاطر، حتــى نصل إلى تحديد وتوثيق

وتقييم الضوابط الداخلية الرئيسـية؛ كل ذلك سيساعد المؤسسة على تحقيق الامتثال للبند ٤٠٤ من قانون ساربنز أوكسلي SOx. أضف إلى ذلك، أنه من خلال الدعم المقدم لكوبت من قبل المنظمة المهنية ITGI والقبول الدولي الواسع النطاق له، يعد وثيقة حية يتم تحديثها من وقت لآخر.

في ظل وجود قانون ساربنز أوكسلي SOx، والتشديد المتزايد على حوكمة تقنية المعلومات، وإدراك مدى أهمية تقنية المعلومات في معظم قرارات الرقابة الداخلية، فقد مر كوبت بعدة مراجعات حتى وصل إلى نسخته الحالية الممثلة بالإصدار الخامس الذي سيتم إطلاقه قريباً. لقد قام معهد حوكمة تقنية المعلومات الراعي لكوبت بعمل رائع هو إصدار مجموعة من المطبوعات التي ترسم علاقة الإطار كوبت مع تلك المعايير الأخرى.

إن المجموعة الكاملة من مواد أهداف الرقابة في كوبت سوف توفر دعماً قوياً لفريق الإدارة الذي يقوم بإجراء مراجعة لتقييم الرقابة الداخلية في ضوء البند ٤٠٤ من قانون SOx. وعلى الرغم من أنه يمكن استخدام هذه المفاهيم في أي مجال من مجالات الرقابة الداخلية، فإن التركيز هنا فقط على تطبيقات وعمليات تقنية المعلومات. وبالنسبة للعديد من المؤسسات فإن فهم وتقييم الرقابة الداخلية المرتبطة بتقنية المعلومات هو المفتاح لتحقيق الامتثال لقانون SOx. وعلى الرغم من أن كوبت موجود منذ سنوات عديدة فإنه ولفترة طويلة كان الكثير ينظر إليه على أنه مجرد أداة متخصصة لتدقيق تقنية المعلومات، ولم يكن يُنظر إليه على أنه يقدم المزيد من المساعدة في أعمال التقييم الأخرى للضوابط الداخلية والتدقيق الداخلي بوجه عام. وعلى الرغم من أن تركيز كوبت لا يزال مُنْصَباً على تقنية المعلومات، فإنه يجب على كبار المديرين أن يقوموا باستكشاف هذا الإطار باعتباره أداة ممتازة للمساعدة في الامتثال للمتطلبات الحالية والمتطورة لقانون SOx.

كوبت في دائرة الضوء:

ينبغي على جميع كبار المديرين المتخصصين سواء في التشغيل أم في المالية أو تقنية المعلومات في المؤسسة أن يكون لديهم على الأقل فهم عالي المستوى لإطار العمل كوبت. فهو بوجه خاص أداة مفيدة وهامة لتقييم نظم الرقابة المالية الداخلية والعمليات الشاملة للحوكمة في بيئة أكثر توجهاً نحو تقنية المعلومات — وهي البيئة التي نواجهها تقريباً اليوم

بشكل دائم. إن قرار استخدام كوبت في عمليات حوكمة تقنية المعلومات لا ينبغي أن يكون مؤقتاً أو قراراً فردياً لأحد كبار المديرين. بل ينبغي على كبار المديرين وكذلك المتخصصين في الرقابة الداخلية والمدققين الداخليين لديهم في المؤسسة القيام بتطوير الأهداف واتخاذ الخطوات اللازمة لتنفيذ إطار العمل كوبت.

يعد كوبت إطار للرقابة الداخلية وأداة تقييم رائعة - وفي بعض الأحيان رائعة للغاية - لوضع عمليات خاصة بحوكمة تقنية المعلومات وتقييم الضوابط الداخلية لها. ولعل أكبر عائق يواجه الإدارة العليا التي تحاول استخدام كوبت بشكل كامل هو أن هذا الإطار قد تم بناؤه في الأصل ليكون بالمقام الأول أداة لتدقيق تقنية المعلومات. على الرغم من أن انتقال رعاية المواد الإرشادية لكوبت من إزاكا إلى ITGI قد أدى إلى توسيع جاذبيتها وتركيزها، فإن هناك تركيزاً كثيفاً جداً على تقنية المعلومات في العديد من هذه المواد المنشورة. ومن المؤكد أن هذا يخيف البعض.

تكمن القوة الحقيقية لكوبت في تركيزه على حوكمة تقنية المعلومات كما هو مبين في الشكل التوضيحي (٥-١). حيث يوضح الشكل أهمية التحالف الإستراتيجي بين الأعمال وموارد تقنية المعلومات إلى جانب إيصال القيمة وإدارة الموارد وإدارة المخاطر وعمليات قياس الأداء. وهذه الأمور تسمح للمؤسسة بتأسيس حوكمة فعالة لتقنية المعلومات، وينبغي أن يساعد كوبت في إدارة وفهم هذه المفاهيم. ولنا أن نتوقع استمرار نمو المعايير والممارسات المنشورة لكوبت والذهاب إلى ما هو أبعد من كونها مجرد مفاهيم أساسية خاصة بـ "تدقيق تقنية المعلومات".

ملاحظات:

١- يقع كلٌّ من معهد حوكمة تقنية المعلومات (ITGI) وجمعية ضبط وتدقيق نظم المعلومات (ISACA) في مدينة رولينج ميدوز بولاية إلينوي الأمريكية.

٢- كوبت ٥: المسودة الخاصة بعرض الإطار (رولينج ميدوز، الينوي، معهد حوكمة تقنية المعلومات، ٢٠١١).

الفصل السادس

إرشادات إطار آيتيل (ITIL) وإدارة خدمات تقنية المعلومات

في الواقـع لم يكـن مفهـوم إدارة خدمـات تقنيـة المعلومـات IT SERVICE MANAGEMENT (ITSM) معروفـاً في الأيـام الأولى لإدارات عمليات تشـغيل تقنية المعلومات الخاصة بمؤسسـات الأعمال. فـإدارة خدمات تقنية المعلومـات ITSM عبارة عن النظام أو الأسـلوب المتبع لإدارة نظم تقنية المعلومات التي تعتمد على رأي العميل في حجم مساهمة تقنية المعلومات في الأعمال. تعمل عمليات إدارة خدمات تقنية المعلومات بشـكل مدروس ومتزن على عكس الأساليب التقنية المركزية التي كانت تستخدم في الماضي لإدارة تقنية المعلومات، وتعد العمليات القوية لإدارة خدمات تقنية المعلومات من العناصر الهامة في الحوكمة الفعالة لتقنية المعلومات.

يستعرض هذا الفصل القضايا الهامة في إدارة خدمات تقنية المعلومات ITSM بالنسبة للحوكمة الفعالة لتقنية المعلومات، وذلك من خلال تعريف كبار محترفي الأعمال المتخصصين لمكتبـة البنية التحتية لتقنيـة المعلومـات Information Technology Infrastructure Library (ITIL)، وهـي عبـارة عن مجموعة من أفضل الممارسـات المتعارف عليها دولياً والتي تغطي معظم الجوانب الخاصة بعمليات تشغيل تقنية المعلومات.

آيتل (ITIL) هو اختصار متعارف عليه ومعترف به للمواد الإرشادية الآخذة في التوسع والتـي وُضعـت لأول مرة في ثمانينيـات القرن الماضي من قبل مكتـب التجارة الحكومية Office of Government Commerce (OGC) التابـع للحكومـة البريطانيـة. وعلى الرغـم من أنهـا كانت في الأصل عبارة عن مكتبة كتب حقيقية، فإنها اليوم تعد مجموعة من أفضل الممارسـات المسـتقلة لتقنية المعلومات والتي يتـم تحديثها بانتظام والتي قد تـم اعتمادها في البداية على نطاق واسـع من قبل عمليات تشـغيل تقنية المعلومات في المملكة المتحدة، ثم تلاها بعد ذلك الاتحاد الأوروبي European Union (EU)، وقد شاع استخدامها الآن بشكل متزايد في الولايات المتحدة الأمريكية. وكما هو الحال تماماً بالنسبة لشركـة آي بي إم (IBM) التـي أصبحت اسـماً بحد ذاتها بدلاً من كونهـا اختصاراً لآلات

الأعمال العالميــة International Business Machines، فــإن معظم المهنيين المحترفين هذه الأيام قد نسوا الكلمات التي يتكون منها ITIL.

آيتل (ITIL) عبارة عن إطار عمل تفصيلي لأفضل الممارســات المهمة لتقنية المعلومات، بما فيه من قوائم مراجعة ومهام وإجراءات ومسؤوليات شاملة تم تصميمها لتتلاءم مع أي إدارة من إدارات تقنية المعلومات. فمن خلال تقســيم العمليات الأساسية الخاصة بتقديم الخدمات إلى عمليات خاصــة بتقديم خدمات تقنية المعلومات وعمليات تعمل على دعم الخدمــات؛ أصبح آيتل الآن في واقع الأمر أســلوباً أو منهجية لوصف العديد من العمليات الأساســية الموجودة في إدارة خدمات تقنية المعلومــات، مثل إدارة التهيئة أو إدارة التغيير. ويحدد إطار آيتل سلسلة من أفضل الممارسات الأساسية التي لا غنى عنها في حوكمة تقنية المعلومات.

تعــد مفاهيم آيتــل هامة بالنســبة للحوكمة الفعالــة للعمليات التشــغيلية في تقنية المعلومات في أي مؤسســة. وبشــكل مغاير تماماً للأيام الأولى لظهور نظم تقنية المعلومات المؤسسية عندما كان يقوم مطورو نظم وإدارات تشغيل تقنية المعلومات ببناء العديد من النظم الرئيســية المرتبطة بتقنية المعلومــات، فإن إدارة خدمات تقنية المعلومات (ITSM) تدعــو مســتخدمي تلك التقنية إلى أن يكــون لهم دور أكبر بكثير في مثــل هذه العمليات الشاملة.

أساسيات آيتل:

آيتل عبارة عن (أو كان في وقت من الأوقات) "مكتبة" رسمية للمطبوعات التقنية، التي نشرت مــن قبل مكتب تجــارة الحكومة البريطــاني[1] British Office of Government Commerce. حيــث يتم التحكم في المطبوعات ومحتوياتها بشــكل محكم، وذلك عــلى غرار مطبوعات المعايير الدولية الصادرة عن الآيزو ISO، والتي تم الحديث عنها في الفصل الســابع من هذا الكتاب. يقدم آيتل إطار عمل لحوكمة تقنية المعلومات يركز على القياس والتحســين المســتمر لجودة خدمــات تقنية المعلومات المقدمة، وذلك من منظور الأعمال والعملاء. وقد كان لهذا التركيز دور رئيــسي في نجــاح آيتل في جميع أنحاء العالم، كما أســهم أيضاً في اســتخدامه وفي الفوائد

الرئيسية التي حصلت عليها المؤسسات التي قامت بنشر تقنيات وعمليات آيتل في جميع أنحاء الإدارات التابعة لهم. وفيما يلي بعض من هذه الفوائد:

- تزايد رضا المستخدم والعميل عن خدمات تقنية المعلومات التي يتم تقديمها.
- تحسين إتاحة الخدمات يؤدي بشكل مباشر إلى تزايد محتمل لأرباح وعائدات الأعمال.
- تحقيق توفيرات مالية نتيجة تقليص تكرار العمل وتقليص الوقت المهدر وتحسين إدارة الموارد واستخدامها.
- تحسين الوقت لتسويق النواحي الخاصة بتقنية المعلومات من منتجات وخدمات جديدة.
- تحسين صنع القرار وتحسين المخاطر لكافة العمليات ذات الصلة بتقنية المعلومات.

تشمل أفضل ممارسات آيتل الخاصة بتقديم الخدمات ما يطلق عليه غالباً مصطلح البنية التحتية لتقنية المعلومات، وهي العمليات الداعمة التي تسمح لتطبيقات تقنية المعلومات بالعمل وتوصيل نتائجها لمستخدمي النظم. في كثير من الأحيان، كانت إدارة المؤسسة تركز اهتماماتها على الجانب التطويري للتطبيقات المرتبطة بعمليات تقنية المعلومات وتهمل الدعم الهام والضروري لعمليات تقديم الخدمات. فمن الممكن على سبيل المثال أن تبذل المؤسسة مجهوداً ضخماً في بناء وتطبيق نظام جديد للتنبؤ بالميزانية، غير أن القيمة الحقيقية المكتسبة من هذا التطبيق أو النظام الخاص بالميزانية ستكون قليلة ما لم تكن هناك عمليات وإجراءات جيدة معمول بها وموضوعة في موضع التنفيذ، كعمليات إدارة المشاكل والحوادث، التي تسمح لمستخدمي هذا النظام (التنبؤ بالميزانية) بأن يقوموا بالإبلاغ عن الصعوبات أو المشاكل التي تواجههم أثناء استخدامهم له. ومن الضروري أيضاً أن تكون هناك عمليات جيدة تتعلق بالسعة والإتاحة لكي تسمح للتطبيق الجديد بالعمل بالشكل المطلوب. إن جميع عمليات الآيتل هذه تعد جزءاً من البنية التحتية لتقنية المعلومات، فالتطبيقات المحكمة والمصممة على نحو جيد تكون قيمتها محدودة بالنسبة لمن يستخدمها في حال عدم وجود مثل هذه العمليات القوية الخاصة بدعم وتقديم الخدمة في موضعها الصحيح.

في الوقت الذي انتشرت فيه أفضل الممارسات آيتل خلال السنوات الأخيرة في العديد من الأماكن الأخرى في العالم، أصبحت الآن أيضاً أكثر قبولاً ومعترفاً بها على نطاق واســع داخل الولايــات المتحدة. تقدم الأجــزاء التالية لكبار المديرين نظرة عامة عــن العمليات الهامة والخاصــة بتقديم الخدمات في آيتل. وهذا من شــأنه أن يقدم بعض الإرشــادات المتعلقة بالكيفيــة التي يجب من خلالهــا أن تمتلك إدارات تقنية المعلومات في المؤسســة عمليات فعالة وفي الموضع المناســب لها، مثل وجود مكتب مســاعدة أو خدمة العملاء، في المجالات المهمة لعمليات تقنية المعلومات. لا يحدد آيتل معايير بعينها لبناء وإدارة الضوابط الخاصة بتقنية المعلومات، ولكنه يقترح طرقاً جديدة لتنفيذ وتشــغيل ضوابط عامة للبنية التحتية التي ينبغي أن يكون معمولاً بها بالفعل.

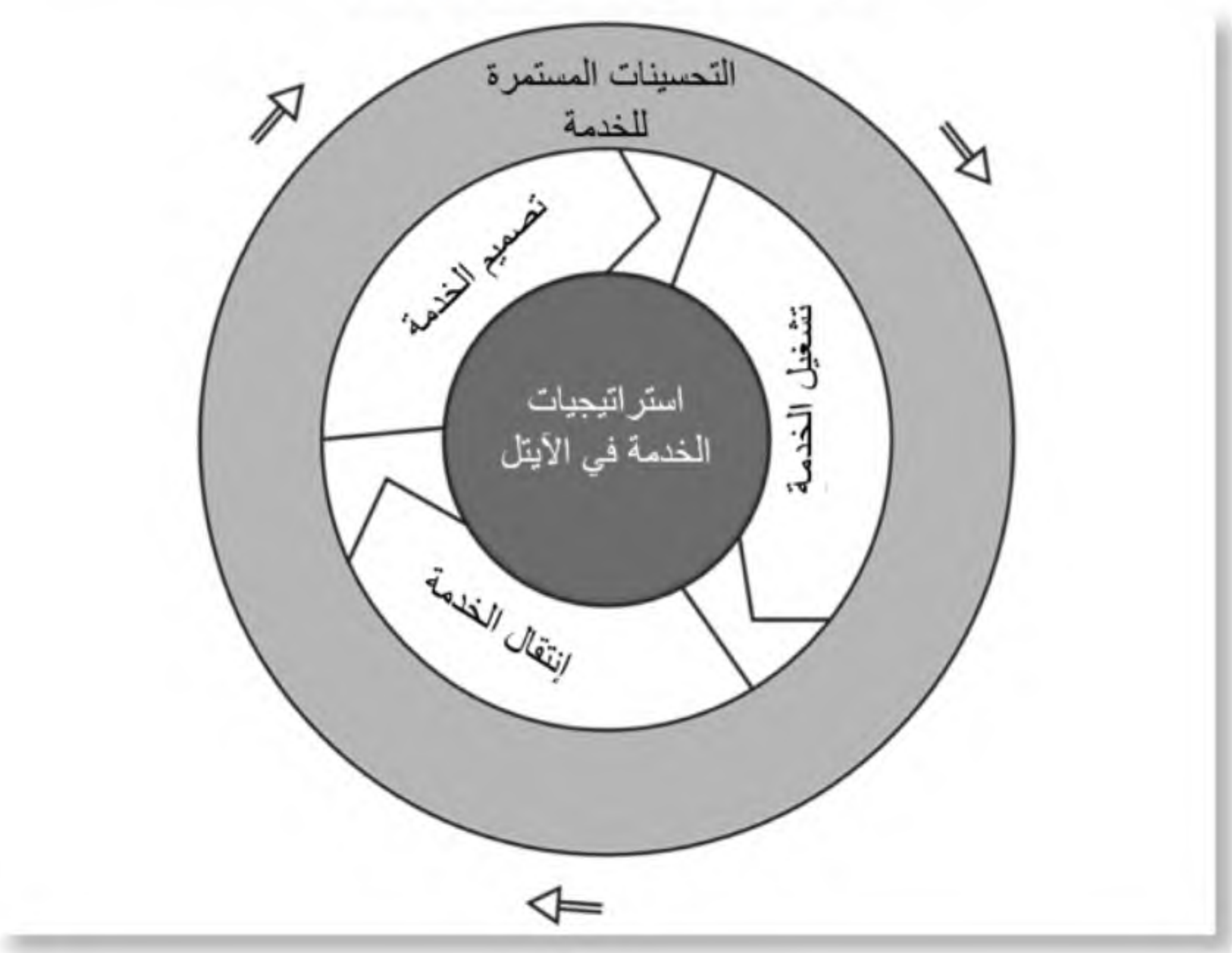
يمكن النظر إلى إســتراتيجيات تقديم الخدمة الموجودة في آيتل على أنها دورة مســتمرة لحياة النشاط، حيث تحتوي هذه العملية على ثلاث أنشطة تم عرضها في الشكل التوضيحي (٦-١) وهــي: تقديم الخدمة ودعم الخدمة وانتقال الخدمة. وســنقوم بمناقشــة كل من هذه الأنشــطة في الأجزاء التالية. إن المبدأ الرئيسي هنا هو أن المؤسســة المستعدة لتطبيق الآيتل ينبغي أن يكون لديها عمليات مســتمرة وجاهزة تتعلق بالخدمات وتتضمن جميع العمليات الأخرى في إدارة الخدمات وتســتقبل مدخلات من مصادر خارجية لعملاء تقنية المعلومات. تقع العملية الخاصة بإســتراتيجية الخدمة في وســط هــذه الحلقات المركزية. حيث تشتمل هذه العملية الأساسية أو المركزية على السياسات والممارسات الخاصة بإدارة تقنية المعلومات والتي تم وصفها في عنصر بيئة الرقابة في إطار الرقابة الداخلية (COSO) والذي تم طرحه في الفصل الرابع من هذا الكتاب. كما يُظهر الشكل التوضيحي (٦-٢) هذا النموذج نفسه الخاص بتقديم الخدمات كعملية لخريطة سير التغذية الراجعة.

وقد جرت العادة على تقســيم عمليــات آيتل إلى عمليات لدعــم الخدمات وعمليات لتقديــم الخدمــات. فعمليات دعم الخدمة تســاعد في جعل تطبيقــات تقنية المعلومات تعمل بطريقة فعالة ومرضية للعميل، في حين تعمل عمليات تقديم الخدمة على تحســين كفــاءة وأداء عنــاصر البنيــة التحتية لتقنية المعلومــات. وهناك خمــس عمليات لأفضل الممارســات المتعلقة بدعــم الخدمات في آيتل والتي تبدأ بالعمليــة التي يطلق عليها إدارة

الإطـلاق Release Management ، وهي المعنية بوضع منتـج تقنية المعلومات في البيئة الإنتاجيـة، إلى أن تصل إلى عملية إدارة الحوادث Incident Management ، وهي المعنية بعمليات الإبلاغ المنتظم عن المشـاكل أو الحوادث الموجودة في تقنية المعلومات. تشـتمل عمليات دعم الخدمة في آيتل على الممارسات الجيدة أو الرشيدة لأي إدارة من إدارات تقنية معلومات مؤسسية، والتي تمتد من عملية التشغيل المركزي القائمة على استخدام الخادم أو النظم التقليدية القديمة للحاسبات المركزية كنقطة تحكم مركزية لتقنية المعلومات الخاصة بها إلى أن تصل إلى العمليات التشغيلية المنتشرة بكثرة لنظم (الخادم - العميل).

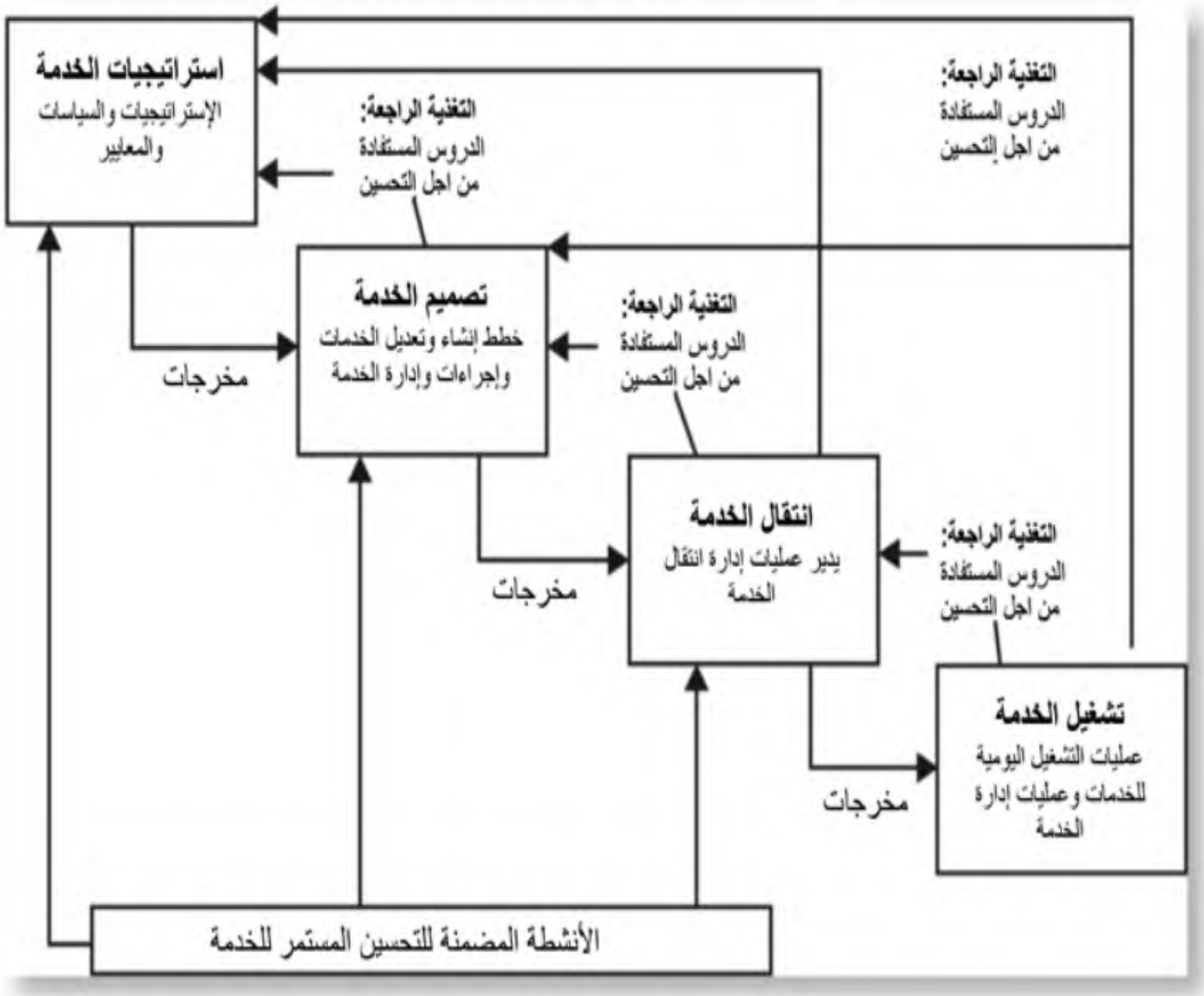
شكل توضيحي (٦-١)

دورة التغذية الراجعة المستمرة في آيتل



شكل توضيحي (٦-٢)

عمليات التغذية الراجعة للخدمة في الآيتل



ونظـراً لوجـود العديد من الاختلافـات المحتملة في إدارة العمليات التشـغيلية لتقنية المعلومـات، فـإن آيتل لم يحـدد التفاصيل المتعلقـة بـ "كيف" يتم تطبيـق عمليات دعم الخدمة مثل إدارة التهيئة أو إدارة التغيير. وإنما يقوم آيتل باقتراح مجموعة من الممارسات والطـرق الجيدة لإدارة المدخـلات والعلاقات بين تلك العمليـات. ولا يوجد أي ترتيب أو أسبقية لأي من هذه الممارسات والطرق. فمن الممكن النظر إليها وإدارتها بشكل منفصل، ولكنهـا جميعاً ترتبـط بطريقة ما بعضها مع بعض. تقدم مجـالات إدارة الخدمة الخاصة بتقديم ودعم الخدمة المتاحة في آيتل إلى جانب إدارة أمن المعلومات، الربط بين العمليات التشغيلية للأعمال وإدارة تقنية المعلومات والبنية التحتية الخاصة بها.

وعلى الرغم من أن هناك العديد من العناصر المستقلة لكنها مترابطة مع آيتل، فإن هذا الفصل سيناقش فقط مكونات دورة حياة الخدمة في آيتل والتي تعد أكثر أهمية بالنسبة للعمليات الفعالة لحوكمة تقنية المعلومات. تقترح أفضل الممارسات في آيتل أساليب مفضلة للعمليات التشغيلية لتقنية المعلومات لتشغيل النظم الإنتاجية لتقنية المعلومات بطريقة تسمح بتعزيز كفاءة العمليات وتقديم خدمات ذات جودة عالية لعملاء أو مستخدمي الخدمات. وتكون هذه الأساليب مفيدة على وجه الخصوص عند إجراء عملية التقييم وتقديم التوصيات في إحدى مجالات العمليات التشغيلية لتقنية المعلومات.

أثناء القيام بمراقبة ومراجعة الضوابط الداخلية لعمليات تشغيل تقنية المعلومات، فإن أحد الطرق التي تكون غالباً مجدية هو التفكير في مجال تقنية المعلومات الذي يجري مراجعته من حيث عمليات الإطار آيتل المستقلة والمذكورة في الأجزاء التالية. على سبيل المثال، فإن إحدى عمليات آيتل التي تسمى إدارة الحوادث، أو التي يطلق عليها عادة "مكتب المساعدة"، هي إحدى الخدمات المساندة أو الوسيلة التي يمكن استخدامها من قبل عملاء ومستخدمي النظم في حال وجود أي استفسار أو مشاكل حول العمليات التشغيلية لتقنية المعلومات. وعلى الرغم من الأهمية القصوى للإدارة الخاصة بمكتب المساعدة، فإنه يكون غالباً مصدر شكوى، مثال على ذلك، طرح المشكلة نفسها عدة مرات دون وجود أي جهود مبذولة بشكل واضح لتحليل الأمور والشروع في حلها. وبالنظر إليه على أنه ليس مجرد كونه مكتب مساعدة تقليدياً، بل على أنه عملية شاملة يتم من خلالها تحويل المسائل إلى عمليات الدعم الأخرى؛ فإن ذلك سوف يحسن أداء وجودة جميع العمليات التشغيلية المتعلقة بتقنية المعلومات في هذه الحالة.

عناصر إستراتيجية الخدمة في آيتل:

يبين الركن العلوي الأيسر من الشكل التوضيحي (٦-٢) الذي يعرض الرسم التخطيطي لعمليات حلقة التغذية الراجعة في آيتل، وظيفة تسمى إستراتيجيات الخدمة. يصف هذا العنصر سياسات وإستراتيجيات ومعايير إدارة الخدمة في آيتل، ويقوم أيضاً بتقديم المدخلات والإرشادات اللازمة للعمليات الأخرى في آيتل وهي تصميم ونقل وتشغيل الخدمة. كما ستقوم تلك العمليات الثلاثة الأخيرة لاحقاً بتقديم المدخلات الضرورية لعملية إستراتيجيات الخدمة لإجراء التحسينات المستمرة عليها.

وكواحدة من أفضل الممارســات الخاصة بحوكمة تقنية المعلومات، يقترح آيتل أن يقوم القائمــون على إدارة تقنيــة المعلومات أولاً بتقييم إســتراتيجية الخدمة الخاصة بهم، وذلك من خلال قيامهم بتوجيه بعض الأســئلة الجادة لأنفسهم والتي تتعلق بجودة خدمة تقنية المعلومات التي يقدمونها والتي تشمل:

- أي من خدمات تقنية المعلومات التي نقدمها أو عروض الخدمة هي الأكثر تميزاً؟
- أي من الخدمات التي نقدمها هي الأكثر ربحية للمؤسسة بأكملها؟
- أي من عملائنا وأصحاب المصلحة هم الأكثر رضا؟
- ما المجالات أو الخدمات التي قد تكون نقاط مشاكل محتملة أو مجالات لعدم الرضا؟
- أي من الأنشطة التي نقوم بها هي الأكثر اختلافاً وفاعلية؟

هذه الأســئلة ليســت من النوعية التي تقــوم إدارة تقنية المعلومات عــادة بتوجيهها، ســواء من الإدارة أثناء قيامها بتقييم موارد تقنية المعلومات لديها أو من قبل الإدارة العليا أو المدققين الداخليين. بل تمثل بعض الأســئلة الهامة التي ينبغي أن تؤخذ بالحســبان من قبل إدارة تقنية المعلومات أثناء قيامها بتقييم إستراتيجيات خدمات تقنية المعلومات التي تقدمها. والفكرة هي تحفيز إدارة تقنية المعلومات في المؤسســة لكي تكون أكثر من مجرد مصــدر للحفاظ على عمليات تقنية المعلومات، بل لتكون أحد المصادر التي تقدم خدمات ذات قيمة عالية للمؤسســة بالكامل وبتكلفة معقولة. الشكل التوضيحي (٦-٣) عبارة عن قائمة لبعض الأســئلة الأخرى التي تساعد إدارة تقنية المعلومات للنظر في قدراتها وعروضها الإستراتيجية وتحسينها.

ســتكون هناك حاجة لاتباع النهج المتعدد التخصصات للقيام بالرد على هذه الأسئلة المطروحة في الشكل التوضيحي (٦-٣)، وذلك بسبب اقتراح آيتل الذي ينص على أنه ينبغي على إدارة تقنيــة المعلومات أن تتعامل مع العديد من الإدارت كالعمليات التشــغيلية، والماليــة، وإدارة الجــودة، والتدقيــق الداخلي لتتمكن من فهم وتحديد الإســتراتيجيات الرئيســية لتقنية المعلومات في المؤسسة بشــكل أفضل. الفكرة كلها هي أنه يجب على قســم أو مجموعة تقنية المعلومات أن يقرروا ما هو وضعهم بالنســبة لكامل المؤسسة،

ومــا الخدمات التي بإمكانهــم أن يقدموها. فقد ينتج عن هذا الأمــر الدليل أو البيان الخــاص بمحفظة الخدمات والذي يقــوم بتحديد القدرات وعــروض الخدمات الخاصة بتقنية المعلومات.

تحــدث الفصــل الخامس من هذا الكتاب عن اســتخدام إطار العمــل كوبت في وضع ضوابــط عامة وفعالة لتقنيــة المعلومات؛ فهذه الأنــواع المقنعة من الضوابــط العامة قد اســتخدمت في جميع العمليات التشــغيلية لتقنية المعلومات في المؤسســة لتوفير الحماية الكافية لجميع النظم والتطبيقات. ومن الممكن أن تكون الأقفال المادية والضوابط الأمنية الأخرى لمركز الخوادم أو النظام الشــائع لأمن تقنية المعلومات القائم على استخدام كلمات المرور والذي يغطي جميع العمليات التشــغيلية لتقنية المعلومات في المؤسســة، أمثلة على تلــك الضوابط العامة. وكما أكد الفصل الرابع عــلى الضوابط الداخلية (COSO)، وكذلك الفصل الخامس، فإن ســوء تنفيذ نظم الرقابة الداخلية لتقنية المعلومات أو ضعفها ســوف يؤثــر في جميع تطبيقــات تقنية المعلومات والتي تعد جزءاً من تلك العمليات التشــغيلية لنظم تقنية المعلومات.

في ظــل ما يشــهده العالم اليوم من الانتشــار الواســع لعمليات ونظم تقنيــة المعلومات الموجودة في جميع أنحاء المؤسسة والتي تمتد من التطبيق الخاص بالتحكم في إحدى عمليات وحدات الأعمال ووصولاً إلى شبكة الإنترنت واسعة الانتشار، فإنه ينبغي أن يكون لدى كل من إدارة المؤسســة والموظفين المعنيين فهم جيد للتقنيات المســتخدمة للرقابة الداخلية في تقنية المعلومات. وعلى الرغم من صعوبة تحديد الخطوط الفاصلة في بعض الأحيان، إلا أننا نستطيع التفكير بشكل عام في ضوابط تقنية المعلومات على مستويين عريضين هما: ضوابط التطبيقات التــي تغطي عملية بعينها (مثل تطبيق مدفوعات الحســابات لدفع فواتير المشــتريات)، وما يطلــق عليه ضوابط عامة لتقنية المعلومات. وتشــتمل هــذه الفئة الأخيرة من الضوابط على العديد من الضوابط التي تتجاوز تلك التي ناقشناها في الفصل الرابع من هذا الكتاب، غير أنها مهمة لجميع جوانب العمليات التشغيلية الخاصة بتقنية المعلومات المؤسسية.

شكل التوضيحي (٦-٣)

أسئلة لتنمية القدرات الإستراتيجية في آيتل

- مـا خدمات تقنية المعلومات التـي ينبغي أن نقدمها؟ ولمن؟ بمعنى، هل نخدم جميع وحدات المؤسسة أو عينة محدودة أو عملاء من الخارج؟
- كيف نميز أنفسنا عن البدائل المنافسة؟ قد يقدم مزودو الخدمات الخارجيين خدمات بديلـة، ولكن ما التكاليف أو القيم الفريدة التـي تجعل إدارة تقنية المعلومات تظهر كبديل أفضل؟
- هل لدى فريق الإدارة إدارات أخرى بديلة لتقديم خدمات تقنية المعلومات من خارج المؤسسة يمكن أخذها في الاعتبار بجدية؟
- كيف يمكننا حقاً خلق قيمة لعملائنا؟ في كثير من الأحيان، تعالج تقنية المعلومات فقط الخدمات المطلوبة مثل تقارير الإقفال المالي في نهاية الشـهر ولكن لا تعالج المعلومات اللازمـة لاتخاذ قـرارات تخص الاسـتجابة السريعة. لذلك ينبغي عـلى مديري تقنية المعلومات التنفيذيين محاولة معرفة كيف يمكنهم خدمة مستخدميهم بصورة أفضل.
- كيف يمكننا وضع محفظة للاسـتثمارات الإسـتراتيجية؟ فبدلاً من مجرد تقديم طلبات الميزانية بانتظام فيما يخص مسائل مثل ترقيات البرمجيات، هل يتم تقييم وتبرير مثل هذه الطلبات بعناية من قبل إدارة تقنية المعلومات؟
- كيف ينبغي أن نحدد جودة الخدمة؟ من خلال المسـوحات والعمل التعاوني، هل كل الأطراف المعنية تدرك مدى الخدمات عالية الجودة التي تقدمها تقنية المعلومات؟
- كيف يمكننا تخصيص مواردنا بكفاءة من خلال محفظة مُعَرَّفة لدينا من الخدمات المقدمة؟
- كيف يمكننا حل الطلبات المتعارضة بالنسبة للخدمات المشتركة؟

وعلى الرغم من أن مفهـوم الضوابط العامة لتقنية المعلومات موجود منذ الأيام الأولى للحاسبات المركزية، فإننا اليوم نستخدم غالباً مفهوم البنية التحتية لتقنية المعلومات للإشارة إلى مجموعة العمليات التي تشـمل جميع العمليات التشغيلية المتعلقة بتقنية المعلومات في المؤسسة. ستكون هناك اختلافات كبيرة جداً بين البنى التحتية لتقنية المعلومات الخاصة

بالعديد من المؤسسات الكبيرة والصغيرة اعتماداً على الحجم النسبي لعملياتها التشغيلية وطبيعة أعمالها بشكل عام. ونظراً للعديد من هذه الاختلافات المحتملة في أنواع وأحجام نظم ومرافق تقنية المعلومات والتي قد تكون ضرورية في هذه الحالة، فإنه في الحقيقة لا يوجد هنا مجموعة واحدة من إجراءات رقابة صحيحة وأخرى خاطئة. ولكن ينبغي على المؤسسة أن تحدد وتطبق مجموعة من أفضل الممارسات التي من شأنها أن تكون بمثابة إرشادات لوضع الضوابط العامة لتقنية المعلومات الخاصة بها.

في جميع الأحوال فإن المفهوم الهام للرقابة الداخلية هنا، يتجاوز غالباً الكيفية التي يتم من خلالها إيصال تقارير تطبيقات تقنية المعلومات والمخرجات الأخرى لتقنية المعلومات ليصل إلى مستخدمي الأعمال لديها. حيث تقوم كل إدارة من إدارات تقنية المعلومات بدعم مجموعة واسعة من عمليات إدارة خدمات تقنية المعلومات التي تم تعريفها بواسطة آيتل والتي تضمنت مجالات مثل إدارة المشاكل (بمعنى أنه كيف تقوم إدارة تقنية المعلومات بحل المسائل والقضايا المتعلقة بمستخدمي الأعمال لديها) وإدارة التهيئة (بمعنى انه كيف تقوم إدارة تقنية المعلومات بمتابعة إصدارات البرمجيات والمعدات المستخدمة لديها والاحتفاظ بها في أحد السجلات). تشتمل إدارة خدمات تقنية المعلومات على عدد كبير من قضايا الرقابة الداخلية، وبدلاً من الحديث عن إيجابيات وأخطاء عملية محددة، فهناك بعض الممارسات المثلى المتعارف عليها والتي يجب على المؤسسة أن تقوم باستخدامها. حيث يعد التطبيق الفعال لأفضل الممارسات الموجودة في آيتل أحد العناصر المهمة في الممارسات الشاملة الجيدة لحوكمة تقنية المعلومات.

تعد الإدارة المالية لخدمات تقنية المعلومات أحد المجالات التي يتم تجاهلها غالباً من قبل الإدارة المالية وإدارة تقنية المعلومات. إن أفضل الممارسات لإدارة الخدمة التي يوصي بها آيتل هي التي تحدد إطار العمل هنا، ويجب على وحدة تقنية المعلومات وإدارتها أن تضع في الحسبان قضايا الإدارة المالية أثناء قيامهم بتقييم مخاطر الضوابط الداخلية لتقنية المعلومات لديهم وتنفيذهم للتنقيحات والتحسينات الفعالة للضوابط العامة لتقنية المعلومات. ونظراً لعدم وجود تعريف محدد بشكل مطلق لما يسمى «أفضل»، فإن البعض يشير إلى تلك الممارسات باسم الممارسات الجيدة فقط.

وعلى الرغم من وجود العديد من إستراتيجيات إدارة الخدمة التي تم تحديدها ووصفها، فإن الإدارة المالية لخدمات ونظم تقنية المعلومات تعد من أفضل الممارسات الهامة لحوكمة تقنيــة المعلومات التي يتم تجاهلها غالباً من قبل الإدارة المالية وإدارة تقنية المعلومات في المؤسسة. وتعد مســألة الإدارة المالية لخدمات تقنية المعلومات واحدة من المجالات التي يتم تجنبها من قبل الأخصائيين المحترفين في تقنية المعلومات بحجة أنهم ليســوا محاســبين ولا يفهمون الأمور التي تتعلق بالمحاســبة باستثناء القيام بوضع ميزانية بسيطة، في حين أن الموظفــين الاعتياديين في الإدارة الماليــة ينظرون غالباً إلى خدمات تقنية المعلومات على أنها قضية تقنية بحتة أو لا تتعدى اهتمامها وضع ميزانية أساسية. في جميع الأحوال، فإن مجال الإدارة الماليــة لخدمات تقنية المعلومات يعد أحد المجالات المهمة في الرقابة الداخلية التي تدعو للقلق وأحد أفضل الممارسات الموجودة في آيتل.

كانت إدارة تقنية المعلومات في معظم المؤسســات تعمــل في أيامها الأولى كخدمة دعم "مجانيــة" بالاضافة إلى نفقاتها التي كانت تُعَالج من خلال الإدارة المركزية وكذلك التكاليف المخصصــة لصالح المســتفيدين دون إيلاء المزيد مــن الاهتمام للتكاليــف المتعلقة بتقنية المعلومــات. فإذا ما أرادت إحدى إدارات المســتخدمين طلب تطبيق جديد، فإنها ســتقوم بالضغــط على الإدارة لتمويل أعــمال التطوير أو شراء حزم البرمجيــات اللازمة وإضافة أي شخص من الأشخاص الذين لا بد من إضافتهم لإدارتها. مع مرور الوقت، بدأت إدارات تقنية المعلومات بوضع عمليات خاصة بتحميل التكاليف المرتبطة بخدمات تقنية المعلومات التي تقدمهــا وأعمال الدعم التي تقوم بها على المســتفيدين، فإنه كان في الغالب ينظر إلى هذه العمليات على أنها سلسلة من المعاملات التي تقوم بجمع "أموال غير حقيقية" حيث لا أحد يولي المزيد من الاهتمام لموضوع التكاليف الفعلية لخدمات تقنية المعلومات وتسعيرها.

أمــا اليــوم، فيجب أن يؤخذ موضوع التكاليف وتســعير خدمات تقنيــة المعلومات في الحســبان وإيلاء المزيد من الاهتمام به. كما يجب أن تعمل إدارة تقنية المعلومات المدارة بشكل جيد كما لو كانت وحدة أعمال تجارية، وتعد الإدارة المالية في آيتل إحدى العمليات الرئيسية الهامة التي تساعد على إدارة الضوابط المالية الخاصة بهذه الوحدة التجارية. إن الهدف من عملية الإدارة المالية في إســتراتيجية الخدمة هو تقديم النصح والإرشــاد الكافي

لإدارة الأصول والموارد المستخدمة في تقديم خدمات تقنية المعلومات على نحو جيد وفعال من حيث التكلفة. حيث من الواجب أن تكون إدارة تقنية المعلومات قادرة على حساب كامل نفقاتها التي تنفقها على خدمات تقنية المعلومات، وأن تقوم بتحميل هذه التكاليف الخاصة بالخدمات التي يتم تقديمها على عملاء المؤسسة المستفيدين منها. وهناك ثلاثة عمليات فرعية مستقلة ومرتبطة بالإدارة المالية في آيتل هي:

١- **وضع ميزانية لتقنية المعلومات** هي عملية توقع وضبط النفقات المالية على موارد تقنية المعلومات. تتضمن عملية تخصيص الميزانية دورة من المفاوضات التي تتكرر عادة كل سنة، لتحديد الميزانيات العامة إلى جانب الرقابة اليومية المستمرة للميزانيات الحالية. إن تخصيص الميزانيات يضمن أن يكون هناك تخطيط وتمويل ملائم للخدمات المناسبة لتقنية المعلومات وأن تعمل تقنية المعلومات في حدود تلك الميزانية خلال هذه الفترة. وسيكون لإدارات الأعمال الأخرى مفاوضات دورية مع تقنية المعلومات لوضع خطط الإنفاق والبرامج الاستثمارية المتفق عليها؛ وهي ما ستحدد في نهاية المطاف الميزانية التي سيتم تخصيصها لتقنية المعلومات.

٢- **محاسبة تقنية المعلومات** هي مجموعة من العمليات التي تُمَكن إدارة تقنية المعلومات من إجراء عملية حسابية كاملة للطريقة التي يتم من خلالها إنفاق أموالها على العملاء والخدمات والأنشطة. ولا تقوم إدارات تقنية المعلومات اليوم دائماً بعمل جيد في هذا المجال. فهي لديها مجموعة واسعة من التكاليف الخارجية، التي تتضمن البرمجيات، والاتفاقيات الخاصة باستئجار المعدات وتكاليف الاتصالات، وغيرها من النفقات، إلا أنه في كثير من الأحيان لا يتم إدارة هذه التكاليف أو الإبلاغ عنها بطريقة جيدة. كما أن لديها ما يكفي من البيانات اللازمة لدفع الفواتير وتقييم بعض التكاليف لمجالات محددة، إلا أن إدارات تقنية المعلومات غالباً ما تفتقر إلى مستوى أكثر تفصيلاً للحسابات، مثل محاسبة التكاليف أو نموذج المحاسبة القائم على النشاط الموجود في مؤسسات الإنتاج الكبرى.

٣- **المطالبة المالية** هي عمليات التسعير وإصدار الفواتير لمطالبة العملاء بالدفع مقابل الحصول على خدمات تقنية المعلومات التي يتم تقديمها لهم. وهذا يتطلب نظاماً محاسبياً سليم لتقنية المعلومات، ويحتاج إلى أن يتم تطبيقه بطريقة بسيطة ونزيهة

ومحكمة جيداً. في بعض الأحيان يتم تقســيم عمليــة المطالبة بالأموال الخاصة بإحدى إدارات تقنية المعلومات بســبب شــدة تعقيد تقارير الفواتــير المتعلقة بخدمات تقنية المعلومات أو بسبب التقنية المتبعة التي يصعب على العديد من العملاء فهمها. تحتاج تقنية المعلومات إلى إصدار تقاريــر واضحة ومفهومة تتعلق بخدمات تقنية المعلومات المســتخدمة بحيث تُمَكِن العملاء من التحقق من تفاصيلها، وفهم ما يكفي للاستفســار عن الخدمات، والتفاوض بشأن التعديلات إذا لزم الأمر.

تقــوم الإدارة المالية لتقنية المعلومات بدعم عملية إســتراتيجية الخدمة من خلال هذه الإجراءات المحددة للتكاليف، والتسعير، والمطالبة. وعلى الرغم من أن هذه العملية للإدارة الماليــة لا تعمــل عموماً على أنها مركز لتحقيق الأرباح، فإنها تســمح لــكل من إدارة تقنية المعلومات وعملائها بالتفكير بشــكل أفضل بالعمليات التشغيلية لخدمات تقنية المعلومات من الناحية التجارية. وقد تسمح عملية الإدارة المالية لإدارة تقنية المعلومات والإدارة بشكل عــام باتخاذ قرارات تتعلق بتحديد الوظائــف، إن وُجِدَت، والتي يجب الإبقاء عليها بداخل الشركة، والوظائف التي يجب إسنادها (تعهيدها) لمقدمي خدمات من خارج المؤسسة.

تسمح عملية الإدارة المالية في آيتل بإجراء تحليل دقيق لتكلفة خدمات تقنية المعلومات التــي يتم تقديمها والعائد المادي منها، كما تســمح لإدارة تقنية المعلومات بوضع وتحقيق أهداف مالية محددة. كما أنها توفر التقارير الخاصة بعمليات إدارة مســتوى الخدمات في الوقت المناسب، الأمر الذي يُمَكِن العملاء من فهم الطرق المتبعة للمطالبات المالية وتسعير الخدمــات. فمن بين جميع عمليــات آيتل الخاصة بدعم وتقديــم الخدمات، تعد عملية الإدارة الماليــة واحدة من أفضل الممارســات في آيتل التي يكــون الاهتمام بها غالباً أقل من المســتوى المطلوب. فالميول التقنية الموجودة لدى الأشــخاص العاملين في تقنية المعلومات يدفعهم إلى التفكير بالإدارة المالية على أنها قضية محاسبية. على الجانب الآخر من العملة، فإن المهنيين العاملين بالمالية والمحاســبة يميلــون إلى التفكير في هذه القضايا على أنها تقنية بحتــة وأنها لا تتعدى مثل هذه المعاملات الخاصة بمحاســبة اســتئجار المعدات أو رســوم اســتئجار المرافق. إن تكاليف وأسعار خدمات تقنية المعلومات تعد من القضايا الهامة في حوكمة تقنية المعلومات.

تصميم الخدمة فى آيتل:

هناك ثلاثة مجالات لعملية إستراتيجية الخدمة في آيتل في دورة حياة خدمة تقنية المعلومات، تبدأ بتصميم الخدمة، وكما هو مبين في الشكل التوضيحي (٦-١). فإن عمليات تصميم الخدمة في آيتل تغطي مجالات أكثر انسجاماً مع عمليات التشغيل السَلِسَة وذات الكفاءة للبنية التحتية لتقنية المعلومات بشكل عام. ويحدد آيتل خمسة جوانب لتصميم الخدمة:

١- تصميم كل خدمة من خدمات تقنية المعلومات التي يتم تقديمها، يشتمل على المتطلبات الوظيفية، والموارد الضرورية والقدرات المتوقعة.

٢- تصميم نظم وأدوات إدارة الخدمة، يتم غالباً تقديمه عن طريق محفظة رسـمية لإدارة وضبط هذه الخدمات خلال دورة حياتها.

٣- تصميم النظم المعمارية والإدارية لتقنية المعلومات يعد أمراً ضرورياً لتوفير الخدمات.

٤- تصميم العمليات يعد أمراً ضرورياً لتركيب وتشغيل وتحسين مجمل العمليات الخاصة بالخدمات.

٥- تصميم أساليب قياس ومقاييس معيارية لعمليات الخدمات والبنية المعمارية لمكوناتها.

إن مـا يقوم آيتل بتعريفه على أنه خدمات العملاء يـدل حقيقة على أن كل إدارة من إدارات تقنية المعلومات تنشـئ الكثير من الخدمات للعمـلاء، وأنه لا بد من إدارة وضبط هذه الخدمات المعروضة من خلال حوكمة تقنية المعلومات المناسـبة واستخدام التقنيات الخاصـة بأفضل الممارسـات. ولدعم عمليـة تقديم خدمات ذات كفـاءة عالية، قام آيتل بتحديد مجموعة محددة من العمليات النوعية. كان البعض منها كعملية إدارة استمرارية أعمال تقنية المعلومات، مفضلاً لدى إدارة تقنية المعلومات ومدققيها على مر السنين. كما أن هنـاك عمليات أخرى مثل اتفاقيات مسـتوى الخدمـة Service Level Agreements (SLAs)، والتـي تحدد الأداء والتوقعات المتفـق عليها بين إدارة تقنية المعلومات وعملائها والتي لا يتم فهمها وتطبيقها دائماً كما ينبغي. وسيتم مناقشة اتفاقيات مستوى الخدمة في الفصل السابع عشر من هذا الكتاب.

إدارة السعة الخاصة بتقديم الخدمة:

تضمن إدارة السعة في آيتل أن تتماشى سعة البنية التحتية لتقنية المعلومات مع احتياجات العمل للحفاظ على المستوى المطلوب من تقديم الخدمات ضمن تكلفة معقولة ومنطقية من خلال مستويات مناسبة للسعة. فمن خلال جمع البيانات المتعلقة بسعة الأعمال والسعة التقنية، ينبغي أن تسفر هذه العملية من عمليات آيتل عن خطة مناسبة للسعة يتم من خلالها تقديم متطلبات خاصة بسعة تقنية المعلومات يمكن تبرير تكلفتها بالنسبة للمؤسسة. وبالإضافة إلى الهدف الأساسي لفهم المتطلبات الخاصة بسعة تقنية المعلومات في المؤسسة وتقديم مقابل لها (متطلبات - مميزات مقابل متطلبات)، فإن إدارة السعة هي المسؤولة عن تقييم المزايا المحتملة للتقنيات الجديدة التي يمكن أن تكون لدى المؤسسة.

تتكون عملية إدارة السعة في آيتل من ثلاث عمليات فرعية هي: إدارة سعة الأعمال وإدارة سعة الخدمة وإدارة سعة الموارد. بالنسبة لإدارة سعة الأعمال فهي عملية طويلة الأجل لضمان أخذ المتطلبات المستقبلية للأعمال بعين الاعتبار ومن ثم التخطيط لها وتنفيذها حسب الحاجة. أما إدارة سعة الخدمة فهي المسؤولة عن التأكد من أن أداء جميع خدمات تقنية المعلومات الحالية يتفق مع المعايير المحددة في اتفاقيات مستوى الخدمة (SLAs). وأخيراً، إدارة سعة الموارد، فهي تركز بصورة أكبر على الناحية التقنية وهي المسئولة عن إدارة المكونات الفردية الموجودة في البنية التحتية لتقنية المعلومات. تشتمل المدخلات المتعددة لتلك العمليات الفرعية الخاصة بإدارة السعة على ما يلي:

- اتفاقيات مستوى الخدمة والخروقات الخاصة بها (وهذا ما سيتم تناوله بمزيد من المناقشة والتفصيل في الفصل السابع عشر من هذا الكتاب).
- خطط وإستراتيجيات العمل.
- الجداول الزمنية التشغيلية، إلى جانب إجراء تغييرات على الجدول.
- قضايا تطوير التطبيقات.
- القيود المفروضة على التقنية وعمليات الاستحواذ.

- حوادث ومشاكل تقنية المعلومات.
- الميزانيات والخطط المالية.

ونظـراً لهذه المدخلات المتعددة، فإن عملية إدارة السـعة تكـون غالباً تحت إدارة مدير واحد مُعين لإدارة السعة، والذي يجب أن يدير عمليات تقنية المعلومات، ويقوم على تطوير وصيانة خطة رسمية لإدارة السعة، وأن يضمن تحديث السجلات الخاصة بالسعة. وبالإضافة إلى ذلك، لا بد من إشراك مدير السـعة في عمليـات تقييم جميع التغيرات ليحدد مدى تأثير التغيرات الجديدة على السعة والأداء. ولا بد من إجراء عملية التحقق من السعة أثناء اقتراح التعديـلات وبعد تنفيذها. كما يجب أن تولي إدارة السـعة اهتمامـاً خاصاً بالتأثير التراكمي للتغيـيرات على مـدى فترة من الزمن والتي يمكن أن تسـبب انخفاضاً في أوقات الاسـتجابة وحدوث مشـاكل في عمليات تخزين الملفات وفي زيادة الطلب على السـعة المسـتخدمة في عمليات المعالجة. وتشتمل المسؤوليات الأخرى المتعلقة بعملية إدارة السعة على بعض مهام مدير نظم الشـبكات ومدير تطوير التطبيقات. فهم المسؤولون عن ترجمة متطلبات العمل إلى السعة اللازمة لتكون قادرة على تلبية هذه الاحتياجات وتحسين أداء تقنية المعلومات.

إن التطبيق الفعال لعملية إدارة السـعة من شـأنه أن يقـدم لإدارة تقنية المعلومات فوائـد، كتقديم ملخص حقيقي عن السـعة المتاحة حالياً، والقدرة على التخطيط المسـبق لحجم السـعة المطلوبة مستقبلاً. ينبغي أن تكون الإدارة الفعالة للسعة قادرة على تقدير أثر التطبيقات أو التعديلات الجديدة على السعة، كما يجب عليها أن تقوم بتقليل التكاليف التي تتماشى مع متطلبات عمليات التشغيل في المؤسسة. إن التخطيط السليم للسعة يمكن أن يقلل بشكل كبير من التكلفة الإجمالية الناجمة عن اقتناء نظام تقنية المعلومات. فعلى الرغم من أن التخطيط الرسـمي للسـعة قـد يتطلب الكثير من الوقـت والموارد البشرية المتمثلـة في فرق عمل داخلية وخارجية، وبرمجيات وأجهزة وأدوات، إلا أن الخسـائر التي يمكـن تكبدها جراء غياب التخطيط للسـعة قـد تكون كبيرة جداً. إن عـدم إتاحة البيئة الإنتاجية للمسـتخدمين الذين يعملون في إدارات الأعمال الحساسـة، والمبالغ الطائلة التي تنفـق على معدات الشـبكات أو الخدمات، والتكاليف المترتبة عـلى عمليات ترقية النظم الموجودة حالياً بالفعل في البيئة الإنتاجية، كل ذلك قد يكون أكثر من مبرر للتكلفة الخاصة

بعملية التخطيط للسـعة. ولأن هذه العملية تعد من العمليات الهامة في آيتل، لذا ينبغي هنا أن تقوم إدارة تقنية المعلومات بأخذ عمليات إدارة السعة المعمول بها والمتعارف عليها في الاعتبار عند قيامها بمراجعة عمليات حوكمة تقنية المعلومات.

يتحدث الفصل التاسـع من هـذا الكتاب عن المزيد من القضايا المتعلقة بإدارة سـعة تقنيـة المعلومـات مـن منظـور الحوسـبة السـحابية Cloud Computing والافتراضية Virtualization. فالحوسـبة السحابية Cloud Computing تشير إلى تلك الموارد الهائلة لتقنيـة المعلومات المتعددة الخوادم التي يتم توفيرها من قبل عدد متزايد من كبار الباعة. فنحـن الآن في عـصر تتوفر فيه المـوارد التخزينية بأثمان رخيصة أكـثر من أي وقت مضى، لـذا فإننا نتحدث هنا عن كمية غير محدودة تقريباً من المـوارد التخزينية الخاصة بتقنية المعلومـات. أما الافتراضية Virtualization فهي مـن الموضوعات الأخرى التي لها علاقة بإدارة السعة وحوكمة تقنية المعلومات التي تم الحديث عنها ومناقشتها في الفصل التاسع من هذا الكتاب؛ حيث يشير مصطلح الافتراضية إلى الأدوات البرمجية التي يمكن من خلالها مشـاركة أو تقاسـم موارد تقنية المعلومات بطريقة لا تجعلنا نشـعر بالقلـق إزاء القيود المفروضة على الموارد في أي جهاز. وقد أسهمت هذه التقنيات في تغيير العديد من الطرق والأسـاليب المستخدمة، ومع ذلك فإن مفهوم إدارة السـعة في آيتل ما زال يعد واحداً من المفاهيم الهامة في مجال حوكمة تقنية المعلومات.

إدارة الإتاحة للخدمات المقدمة:

ازداد اعتماد المؤسسات هذه الأيام على خدمات تقنية المعلومات المقدمة إليها والمتاحة سـبعة أيام في الأسبوع و٢٤ ساعة في اليوم. في كثير من الحالات نرى أنه عندما تكون تلك الخدمـات الخاصـة بتقنية المعلومات غير متاحة، فإن الأعمال أيضـاً تتوقف. ولذلك فإن قيـام إدارة تقنيـة المعلومات بإدارة ومراقبة مدى إتاحة الخدمـات التي تقدمها تعد من الأمور الحيوية. ويمكن تحقيق ذلك من خلال تحديد احتياجات الأعمال المتعلقة بموضوع إتاحة خدمات تقنية المعلومات، ومن ثم مقارنتها مع الإمكانيات المتوفرة لدى إدارة تقنية المعلومات.

تعتمد أفضل الممارسات الخاصة بإدارة الإتاحة في آيتل على عدة مدخلات، تتضمن المتطلبات المتعلقة بإتاحة الأعمال؛ معلومات عن الموثوقية أو الاعتمادية، والصيانة، والتعافي، وإمكانية تقديم الخدمة؛ ومعلومات من العمليات الأخرى والحوادث والمشاكل ومستويات الخدمة التي يتم تحقيقها. تتمثل أهداف عملية إدارة إتاحة الخدمات في:

- وضع خطة مناسبة ومحدثة لإتاحة الخدمات وصيانتها بحيث تعكس الحاجات الحالية والمستقبلية للمؤسسة.
- توفير الخدمات والإرشادات التوجيهية لكافة المجالات الأخرى في المؤسسة فيما يخص القضايا المتعلقة بإتاحة تقنية المعلومات.
- التأكد من أن الإنجازات التي تتعلق بإتاحة الخدمات تلبي الأهداف الموضوعة وزيادة، وذلك من خلال إدارة أداء الإتاحة بالنسبة للخدمات والموارد.
- المساعدة في تشخيص وحل الحوادث والمشاكل المتعلقة بالإتاحة.
- تقييم تأثير كل التغيرات على خطة الإتاحة والأداء والسعة لجميع الخدمات والموارد.
- ضمان تطبيق الإجراءات الوقائية في أي مكان تكون فيه تكلفة تلك الإجراءات مبررة.

ويمكن وصف الأنشطة المتعلقة بإدارة إتاحة الخدمات على أنها عبارة عن إجراءات للتخطيط والتحسين والقياس. حيث يتضمن نشاط التخطيط القيام بتحديد متطلبات الإتاحة لمعرفة ما إذا كان هناك إمكانية للوفاء بها والكيفية التي يمكن من خلالها تطبيق الإتاحة المطلوبة. إن عملية إدارة مستوى الخدمة، والتي سيتم تناولها بمزيد من التفصيل لاحقاً في الفصل السابع عشر من هذا الكتاب تعد من العمليات التي تبقى على تواصل مستمر بالأعمال والقادرة على تزويد إدارة الإتاحة ببعض التوقعات المناسبة بخصوص الإتاحة المطلوبة. قد يكون هناك توقعات غير واقعية في الأعمال بخصوص إتاحة تقنية المعلومات دون فهم ما يعنيه هذا من حيث القيمة الحقيقية. فمثلاً، قد يرغب مستخدمو الأعمال في توفير إتاحة بنسبة ٩٩٫٩٪، وهم حتى الآن لا يدركون أن تكلفة هذا الأمر ستزيد بمقدار خمسة أضعاف تكلفة الإتاحة التي تتوفر بنسبة ٩٨٪ فقط. وتقع إدارة مثل هذه التوقعات على عاتق إدارة مستوى الخدمة وعملية إدارة الإتاحة.

الشــكل التوضيحي (٦-٤) يوضح العلاقة بين الإتاحة والتكاليف. حيث يتضح أن الحفاظ على مســتوى أســاسي منخفض من الإتاحة الخاصة بتشغيل نظم تقنية المعلومات لن يكلف الكثير، في حال كانت تلك الإتاحة هي كل ما ستحصل عليه المؤسسة. ويجب على إدارة تقنية المعلومات أن تضع هذه العلاقة في الحسبان عند قيامها بمراجعة الضوابط وتقديم التوصيات.

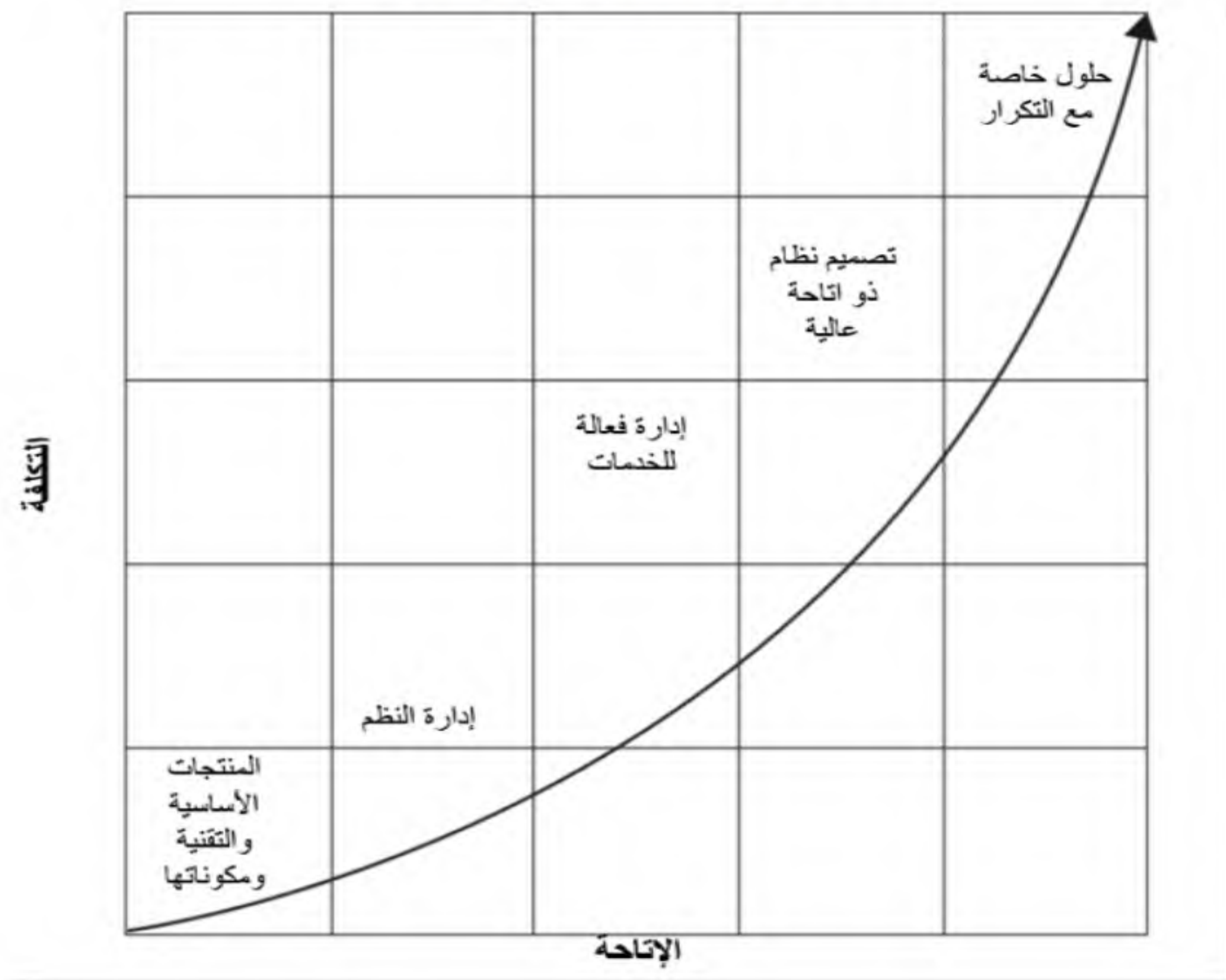
تستطيع إدارة تقنية المعلومات أن تقوم بتصميم إما عملية "إتاحة Availability" الخدمات أو عمليــة "اســترجاع Recovery" الخدمــات. فعندما لا تحتمل الأعمال بقــاء خدمة معينة معطلة لأي فترة من الزمن، فستكون إدارة تقنية المعلومات بحاجة إلى تعزيز المرونة في البنية التحتيــة التقنية الخاصة بها وضمان تنفيذ عمليات صيانة وقائية للمحافظة على اســتمرارية عمل الخدمات. وفي كثير من الحالات قد يكون بناء "إتاحة اضافية" "extra availability" في البنية التحتية مهمة باهظة الثمن ولكن يمكن تبريرها باحتياجات العمل. إن عملية التصميم لإتاحة الخدمات هي عبارة عن نهج استباقي لتفادي تعطل خدمات تقنية المعلومات.

أما إذا كانت الأعمال تستطيع تحمل توقف الخدمات لبعض الوقت، أو عندما لا يكون هناك أي مبررات لعمليات تعزيز إضافية في مرونة البنية التحتية التقنية، فإن وضع تصميم مناســب لاسترجاع الخدمات ســيكون هو النهج المناســب. وفي هذه الحالة سيتم تصميم البنية التحتية بحيث أنه في حال توقف الخدمة ســتبدأ عملية الاســترجاع في استعادة هذه الخدمة وتشــغيلها "في أسرع وقت ممكن". إذ إن وضع تصميم للاسترجاع يعد نهجاً إدارياً للإتاحة يعتمد بشكل كبير على رد الفعل. فعند وقوع أي حادث يجب أن تكون العمليات الأخــرى في آيتل مثــل إدارة الحوادث في موضــع التنفيذ للقيام بعملية اســترجاع الخدمة وتشغيلها بأسرع ما يمكن في حال توقفها أو انقطاعها.

إن الفائدة الرئيســية من إدارة الإتاحة هو امتلاك عملية منظمة لتقديم الخدمات التي يتم توفيرها وفقاً لحاجات العملاء المتفق عليها مسبقاً. الأمر الذي يجب أن يؤدي إلى زيادة إتاحة خدمات تقنية المعلومات وزيادة مســتوى الرضا لدى العملاء. وهذا يغطي مساحة قد تسمح للمدققين على أعمال تقنية المعلومات بطرح بعض الأسئلة الصعبة على أنها جزء من عمليات مراجعة الضوابط العامة لتقنية المعلومات التي يقومون بها.

شكل توضيحي (٦-٤)

العلاقة بين الإتاحة والتكاليف في الآيتل



إدارة أمن واستمرارية نظم المعلومات الخاصة بتقديم الخدمة:

تمثل إدارة الأمن والاستمرارية عنصرين مستقلين من العناصر الخاصة بأفضل ممارسات تقديم الخدمة الموجودة في آيتل. ونظراً لاعتماد الأعمال الآن على تقنية المعلومات أكثر من أي وقت مضى، فإن حجم التأثير الناجم عن عدم إتاحة أي خدمة من خدمات تقنية المعلومات قد يزداد بشكل كبير. وفي كل مرة يتم فيها انخفاض مدى إتاحة الخدمات أو أدائها، لا يستطيع عملاء تقنية المعلومات مواصلة تنفيذ أعمالهم بالشكل الطبيعي. وهذا الاتجاه نحو الاعتماد الكبير على دعم تقنية المعلومات وخدماتها سوف يستمر وسيؤثر بشكل مباشر ومتزايد على العملاء والمديرين وصناع القرار. وتؤكد إدارة الاستمرارية في آيتل أنه يجب تقدير مدى تأثير الفقد الكلي أو الجزئي لخدمات تقنية المعلومات، كما

يجب عليها أيضاً أن تقوم بوضع خطط استمرارية لضمان أن الأعمال، والبنية التحتية لتقنية المعلومات الداعمة لها، سوف تكون قادرة دائماً على الاستمرار في العمل.

يدعو آيتل إلى تطوير إستراتيجية مناسبة تحتوي على شيء من التوازن المثالي بين الخيارات المتعلقة بالحد من المخاطر وخيارات استرجاع الخدمات. وهذه الإستراتيجيات تشبه إلى حد ما بعض الإستراتيجيات الخاصة باستمرارية الأعمال والتعافي من الكوارث المذكورة في الفصل العاشر من هذا الكتاب. وباستخدام الأساليب المذكورة هناك، فإنه يجب على المنظمة أن تقوم بتطبيق مجموعة فعالة من العمليات الخاصة باستمرارية الخدمة.

أما إدارة أمن تقنية المعلومات فهي مجموعة أخرى من أفضل الممارسات في آيتل. فآيتل يقر بضرورة توفر عمليات لأمن المعلومات ضمن إطار حوكمة الشركات، وذلك لوضع توجه إستراتيجي للأنشطة الأمنية وضمان تنفيذ هذه الأنشطة. ويأتي أمن المعلومات كثيراً بعد التركيز على حوكمة تقنية المعلومات، حيث يؤكد آيتل أن أمن المعلومات أكثر من مجرد قضية تخص تقنية المعلومات، فهو أيضاً قضية إدارية. إن أهداف أمن تقنية المعلومات هي حماية مصالح أولئك الذين يعتمدون على المعلومات التي تقدمها تقنية المعلومات وحماية النظم والاتصالات المستخدمة لإيصال تلك المعلومات. ويتم تحقيق أمن المعلومات في آيتل من خلال الأهداف التالية:

- **هدف الإتاحة:** أن تكون المعلومات متاحة ويمكن استخدامها عند الطلب، وأن النظم التي تتيحها يمكنها أن تقاوم وبشكل مناسب الهجمات وتتعافى من الأعطال أو تمنع حدوثها.
- **هدف السرية:** يتم مراقبة المعلومات أو الكشف عنها فقط لأولئك الذين لديهم الحق في الاطلاع عليها.
- **هدف النزاهة أو السلامة:** أن تكون المعلومات كاملة ودقيقة ومحمية ضد التعديل غير المصرح به.
- **هدف الموثوقية وعدم التنصل:** أن تكون إجراءات الأعمال وكذلك تبادل المعلومات بين المؤسسات أو مع الشركاء يمكن الوثوق بها.

وتستمر إدارة أمن المعلومات في آيتل في تحديد أفضل الممارسات للوصول إلى نظام كامل لإدارة أمن المعلومات. فأفضل الممارسات الهامة جداً، والعمليات الفعالة لإدارة أمن المعلومات تشكل عنصراً هاماً من عناصر الحوكمة الفعالة لتقنية المعلومات.

عمليات إدارة انتقال الخدمة في آيتل:

كما يعلم مديرو ومحترفو تقنية المعلومات، أن العمليات التشغيلية الخاصة بتقنية المعلومات تكون دائماً عرضة للتغيرات الدورية التي تتم على المعدات والبرمجيات. وقد تنطوي هذه العمليات على تخطيط الانتقال السليم لإدخال مكونات جديدة، واختبارها والتحقق من صحتها قبل أي إطلاق لها في البيئة الإنتاجية، وكذلك إدارة التهيئة لمراقبة المخزون، والعلاقات بين أجهزة وخدمات تقنية المعلومات. وقد قام آيتل بتجميع هذه الممارسات تحت ما يطلق عليه اسم إدارة الانتقال، وهو المجال الذي يمكن أن يسلط الضوء على بعض مخاطر الرقابة الداخلية المؤثرة بالنسبة للعمليات التشغيلية للبنية التحتية لتقنية المعلومات. فمن الممكن على سبيل المثال أن يتم تثبيت أحد تطبيقات تقنية المعلومات بضوابط داخلية غير مرنة. فضلاً عن أنه، من الممكن أن تتسبب التغيرات اللاحقة غير المصرح بها على التطبيق نفسه أو التهيئة غير السليمة للمعدات الملحقة به بظهور مخاوف رقابية جديدة.

إدارة التغيير الخاصة بانتقال الخدمة:

ينتج غالباً عن عملية إدارة المشاكل التي تم الحديث عنها كجزء من العمليات التشغيلية للخدمات، الحاجة لإجراء بعض التغييرات أو التعديلات في تقنية المعلومات، كالتغيرات التي تطرأ على البرنامج أو التعديلات الطارئة على العملية أو الإجراء لتحسين الخدمات والحد من التكاليف. إن الهدف من إدارة التغيير في آيتل هو استخدام أساليب وإجراءات معيارية للتعامل الفعال والفوري مع التغييرات كافة، وذلك للتقليل من درجة تأثير تلك التغيرات في جودة وأداء الخدمات والعمليات يوماً بعد يوم. وتشمل عمليات إدارة التغيير في آيتل:

- معدات وبرمجيات نظم تقنية المعلومات.
- معدات الاتصالات والبرمجيات.
- جميع برمجيات التطبيقات.
- جميع الوثائق والإجراءات المتعلقة بعمليات تشغيل ودعم وصيانة النظم الحية.

وتعــد النقطــة الأخيرة مصدر قلق واهتمام بشــكل خــاص، إذ يتم غالبــاً تغيير أجهزة وبرمجيات تقنية المعلومات مع عدم الاهتمام بشكل كاف بتغيير الوثائق والبرامج الداعمة المرتبطــة بتلك الأجهــزة والبرمجيات. فالتغــيرات التي تحدث عــلى أي عنصر من عناصر تقنيــة المعلومات (مثل برمجيــات التطبيقات أو الوثائق أو الإجــراءات) يجب أن تخضع لعملية رســمية خاصة بإدارة التغيير. ومع ذلك تكون عملية إدارة التغيير غالباً عشــوائية حتى في أحســن أحوالها. ومــن الأمثلة على ذلك، أن تتم التغيــيرات على التطبيقات دون التفكير في آثارها على مجمل البنية التحتية لتقنية المعلومات، أو بروز تغيرات أخرى ناجمة عــن الإصلاحات التي تقــوم بها إدارة الحــوادث، أو طلبات الإدارة العليــا المتعلقة بإجراء بعض التغيرات اللازمة لحل بعض المشــاكل قصيرة الأجل أو الفورية. لذا ستعمل العمليات الرســمية لإدارة التغيير، والتي تقوم بمراجعة واعتماد التغيرات المقترحة، بشكل مستمر على تحسين عمليات تقنية المعلومات وعمليات الرقابة الداخلية في المؤسسة. وينبغي الربط بين عملية إدارة التغيير الموجودة في آيتل وإدارة التهيئة، التي تم الحديث عنها ســابقاً، بشــكل وثيــق، وذلك لضمان إتاحــة المعلومات الخاصة بالآثار المحتملــة أو المترتبة على التغييرات المقترحة، والكشف عن أي تأثيرات محتملة وعرضها بشكل مناسب.

يجــب أن يكــون لعمليــات إدارة التغيير رؤية عاليــة وقنوات اتصــال مفتوحة من أجل تعزيز الانتقال الســلس عند حدوث التغييرات. ولتحســين هذه العمليــة، قامت العديد من إدارات تقنية المعلومات بتشــكيل مجلس استشــاري رســمي للتغيــير Change Advisory Board (CAB) مكون من مزيج من الأشــخاص العاملين في إدارات تقنية المعلومات وإدارات المستخدمين الأخرى الموجودة بداخل المؤسســة، ليقوموا جميعاً بمراجعة التغييرات والموافقة عليهــا. فالمجلــس الاستشــاري للتغيــير(CAB) هو كيان موجــود للموافقة عــلى التغييرات والمســاعدة في تقييمها وتحديد أولوياتها. ويجب أن يُســنَد للمجلس مسؤولية التأكد من أن جميــع التغييرات قد تم تقييمها بصورة كافية من منظور الأعمال والمنظور التقني. ولتحقيق هذا المزيج، يجب أن يكون المجلس الاستشــاري للتغيير CAB مكوناً من فريق يعي بشــكل جيــد احتياجات أعمال العملاء إلى جانب الوظائــف التقنية الخاصة بالدعم والتطوير. يرأس المجلس الاستشاري للتغيير (CAB) مدير مسئول عن عمليات التغيير، ويجب أن يضم المجلس كلاً مــن عملاء تقنية المعلومات، ومطوري التطبيقات، ومختلف الخبراء/ الاستشــاريين الفنيين

إذا اقتضـت الحاجة ذلـك، وممثلين عن المقاولـين أو الأطراف الخارجية في حـال كان هناك اسـتعانة بمصادر خارجيـة. وعلى الرغم من أنه يجب على هذ المجلـس أن يعقد اجتماعات دوريـة منتظمة لمراجعة وجدولة التغييرات المقترحة، فإنه لا ينبغي أن يكون بمثابة عائق أمام العمليات التشغيلية لتقنية المعلومات، بل لا بد من وجود هذا المجلس لتوفير جدولة منظمة وإدخال جميع أنواع التغييرات على البنية التحتية لتقنية المعلومات.

تحتاج العمليات الشـاملة الفعالة لإدارة الخدمات إلى القدرة على تغيير الأمور بطريقة منظمة، لتفادي الوقوع في أخطاء واتخاذ قرارات خاطئة. إن العملية الفعالة لإدارة التغيير أمر لا غنى عنه بالنسبة لبنية تحتية فعالة لتقنية المعلومات، وينبغي أن تشمل ما يلي:

- تحسين المواءمة والانسجام بين خدمات تقنية المعلومات ومتطلبات العمل.
- الشفافية المتزايدة ووضوح الرؤية والتواصل بشأن التغييرات لكل من فريق دعم الأعمال والخدمات.
- تحسين تقييمات المخاطر.
- تقليل التأثير السلبي للتغيرات على جودة الخدمات.
- تقييم أفضل لتكاليف التغييرات المقترحة قبل أن يتم تكبد تلك التكاليف.
- زيـادة إنتاجية عملاء تقنية المعلومات من خـلال تقليل أوقات الانقطاع وخدمات عالية الجودة.
- زيادة قدرة تقنية المعلومات لاستيعاب حجم كبير من التغييرات.

إن عمليـة إدارة التغيـير في آيتـل تعد عنصراً هاماً مـن عناصر البنيـة التحتية لتقنية المعلومات، وينبغي أن ترتبط وتتماشى بشـكل وثيق مع العمليات الرئيسـية لإدارة التهيئة والسـعة والإطـلاق في البنية التحتية لتقنية المعلومات. وهـي أيضاً عنصر هام من عناصر الحوكمة الفعالة لتقنية المعلومات.

إدارة التهيئة الخاصة بانتقال الخدمة:

مهما كان حجمها النسبي، فإن الإدارات الخاصة بتشغيل تقنية المعلومات تعتبر معقدة، وذلك في ظل وجود العديد من الأنواع والإصدارات الخاصة بالمكونات المادية والبرمجية، هذا بالإضافة إلى الروابط المستخدمة للاتصال بمكونات الحوسبة السحابية، التي يجب أن تعمل جميعها معاً بطريقة منظمة ومحكمة الإدارة. ومن المؤكد أن هذا صحيح بالنسبة للشركة التي تعمل من خلال نظم أجهزة الحاسب المركزية Mainframs التقليدية، أو"مزارع" الخوادم "Farms of Servers"، وعدد كبير من أجهزة التخزين ومعدات الاتصالات، والأمر نفسه يسري على وحدة التشغيل الصغيرة لنظم تقنية المعلومات. تعد الوظيفة الرسمية لإدارة التهيئة عملية هامة لتقديم الخدمات التي تدعم التعريف والتسجيل والإبلاغ عن مكونات تقنية المعلومات وإصداراتها ومكوناتها التأسيسية وعلاقاتها. فالعناصر التي يجب أن تخضع لرقابة إدارة التهيئة تشمل الأجهزة والبرامج والوثائق المرتبطة بها. هناك اختلاف بين مفهوم إدارة التهيئة والمفهوم الخاص بعملية المحاسبة الإهلاكية الخاصة بإدارة الأصول، على الرغم من وجود علاقة بينهما. فنظم إدارة الأصول تحتفظ بتفاصيل عن معدات تقنية المعلومات التي تزيد قيمتها عن حد معين، ووحدة العمل والمواقع التي توجد بها. في حين تحتفظ إدارة التهيئة أيضاً بمعلومات عن العلاقات الموجودة بين الأصول، والتي لا تحتفظ بها إدارة الأصول عادة. فبعض المؤسسات تبدأ بإدارة الأصول ومن ثم تنتقل إلى إدارة التهيئة.

إن النشاط الأساسي والمهم لحوكمة تقنية المعلومات فيما يخص إدارة التهيئة هو تحديد المكونات المستقلة المختلفة للعمليات التشغيلية لتقنية المعلومات، والتي يطلق عليها اسم عناصر التهيئة (CIs)، ومن ثم تحديد البيانات الرئيسية الداعمة لهذه العناصر (CIs)، متضمناً ذلك "أصحابها"، وتحديد البيانات، وأرقام الإصدارات وكذلك العلاقات المتبادلة للنظم. ولا بد من الحصول على هذه البيانات وتنظيمها وحفظها في قاعدة بيانات تُعرف باسم قاعدة بيانات إدارة التهيئة Configuration Management Database (CMDB). ويجب على الفريق المسؤول عن إدارة التهيئة أن يقوم باختيار وتعريف هياكل التهيئة الخاصة بعناصر تهيئة البنية التحتية بأكملها، متضمناً ذلك تحديد العلاقات الموجودة بين

جميـع عناصر التهيئـة (CIs) والمكونات المتصلة في التهيئة الخاصـة بمجمل البنية التحتية لتقنيـة المعلومات. وبالانتقال إلى ما هو أبعد من مجـرد عملية إدخال البيانات في قاعدة بيانـات إدارة التهيئـة، فإنه يجـب أن تضمن العملية أن عناصر التهيئـة المصرح بها فقط هـي التـي يتم قبولها، كما يجب أن تضمن أيضاً عدم إضافـة أي عنصر من عناصر التهيئة أو تعديلـه أو اسـتبداله أو إزالته دون أن يكون هناك طلب سـليم واضـح لإجراء التغيير وبمواصفات محدثة.

يجـب علينا التفكير في أهمية عمليـة إدارة التهيئة من حيث وجود التطبيقات الخاصة بتقنية المعلومات في إدارة الأعمال التقليدية. فربما يكون لدى كل عضو من أعضاء الطاقم الوظيفي هاتف ذكي أو جهاز حاسـب محمول، وفي حال عدم وجود إصدارات متناسقة من البرامـج الموضوعة على كل جهاز مـن هذه الأجهزة، فمن الممكن أن تكون هناك صعوبات في عمليـة اتصال تلك النظم بعضها مع بعض. هذا يفسر أهمية إدارة التهيئة. فمن المهم حقاً أن يكون لديك فهم لمختلف الإصدارات أو حتى الأنواع المتعددة للبرمجيات والمعدات في إدارات التشغيل الكبيرة لتقنية المعلومات.

تتضمن عملية إدارة التهيئة عناصر تحكم مهمة بالنسـبة لمجمل عملية حوكمة تقنية المعلومـات الفعالـة. لذا يجب أن يحتفظ فريق تقنية المعلومات والمسـؤول عن عملية إدارة التهيئة بسـجلات عن حالة كل عنصر من عنـاصر التهيئة (CI) وتتبع حالته عندما تتغـير من حالة لأخرى، فعلى سـبيل المثـال، قد تتغير حالة العنصر مـن مرحلة التطوير إلى مرحلـة الاختبار، ومن ثم إلى مرحلة الإنتاجية، ومن ثم إلى مرحلة الإيقاف أو سـحبه في نهايـة الأمـر. تعد قاعدة بيانات إدارة التهيئة مسـتودعاً لعنـاصر التهيئة، وليس من الضروري أن تكون قاعدة البيانات عبارة عن تطبيق معقد ومتخصص. فمثلاً، يمكن لأي مؤسسـة أن تقوم بإنشاء قاعدة بيانات بسـيطة لإدارة التهيئة CMDB فقط باستخدام جداول البيانات أو باستخدام نظم قواعد البيانات المحلية. وفي ظل وجود البنية التحتية الكبـيرة والمعقـدة لتقنية المعلومـات اليوم، فـإن إدارة التهيئة تتطلب غالباً اسـتخدام المكتبات الطبيعيـة والإلكترونية جنباً إلى جنب مع قاعدة بيانات إدارة التهيئة للاحتفاظ بنسـخ محددة لجميع البرامج والوثائق الداعمة. وينبغي أن تسـتند قاعدة بيانات إدارة

التهيئة إلى تقنية قاعدة البيانات التي توفر وسائل استعلام مرنة وقوية وتحدد العلاقات بين جميع مكونات النظام.

ترتبط عملية إدارة التهيئة مباشرة بعمليات إدارة تطوير واختبار وتغيير وإطلاق النظم للجمع بين المنتجات الجديدة والمحدثة. وبالإضافة إلى ذلك، فإن قاعدة بيانات إدارة التهيئة CMDB يمكن استخدامها من قبل عملية إدارة مستوى الخدمة للاحتفاظ بتفاصيل الخدمات وربط هذه الخدمات مع مكونات تقنية المعلومات التابعة لها. كما يمكن أيضاً أن تُستخدم قاعدة بيانات إدارة التهيئة لتخزين تفاصيل المخزون الخاصة بعناصر التهيئة CIs، مثل المُورِد، والتكلفة، وتاريخ الشراء، وتاريخ تجديد الترخيص. كما أن هناك ميزة إضافية تتمثل في استخدام قاعدة بيانات إدارة التهيئة لتغطية الجوانب القانونية المرتبطة بالحفاظ على التراخيص والعقود.

عمليات تشغيل الخدمة في آيتل:

لقد بدأت أفضل ممارسات آيتل الموصوفة في هذا الفصل بأهمية وضع إستراتيجيات للخدمة، والتي تتضمن السياسات الرئيسية لتقنية المعلومات والمجالات ذات المستوى العالي كالإدارة المالية لتقنية المعلومات. أما بالنسبة للعملية الاعتيادية الخاصة بإطلاق موارد تقنية المعلومات، فإن المجموعة التالية من أفضل الممارسات تغطي تصميم الخدمة، وهي العمليات التي تتناول سعة وإتاحة تقنية المعلومات، وكذلك إدارة مستوى الخدمة لتتفق مع مستخدمي خدمات تقنية المعلومات فيما يتعلق بالخدمات التي سيتم تقديمها. ويطلق على هذه العمليات الثلاث الأخيرة في آيتل اسم عمليات تشغيل الخدمة، وهي العملية التي تتيح لعملاء الأعمال رؤية جودة خدمات تقنية المعلومات التي يتم تقديمها.

تتضمن العمليات التشغيلية للخدمات القيمة اليومية للخدمات التي ينبغي تقديمها بواسطة نظم وعمليات تقنية المعلومات. إن الغرض من عملية تشغيل الخدمة في آيتل هو المساعدة في تنسيق وتقديم خدمات تقنية المعلومات للعملاء. كان هذا هو مفهوم القيمة الذي كان غالباً مفقوداً في الأيام الأولى لعمليات تشغيل تقنية المعلومات، إلا أن أفضل الممارسات في آيتل قد قامت بتقريب هذه المفاهيم المتعلقة باحتياجات العمل والإدارة.

تحدد عمليات تشـغيل الخدمة في آيتل عمليات منفصلة لتشـغيل الخدمة، وذلك فيما يخــص إدارة الأحداث events والحوادثincidents ، حيث يتم تعريف الأحداث على أنها أي واقعــة يمكن اكتشـافها ويكون لها تأثـير في إدارة البنية التحتية لتقنيــة المعلومات أو تقديــم الخدمات المتعلقة بتقنية المعلومات. وعلى الرغم مــن أن آيتل يحدد العديد من أوجه الشـبه بين ما يســمى الأحداث والحوادث في آيتل إلا أن نقاشنا هنا سوف يركز على إدارة الحوادث (الأعطال)، ذلك أن التنفيذ الفعال لهذه العمليات سوف يحسن من مجمل عمليات التشغيل الخاصة بحوكمة تقنية المعلومات.

إدارة الأحداث والحوادث الخاصة بتشغيل الخدمة:

تتضمــن عمليــات إدارة الحوادث جميع الأنشــطة اللازمة لاســتعادة خدمــات تقنية المعلومات بعد انقطاعها. يعرف آيتل الانقطاع أو العطل على أنه أي نوع من أنواع المشاكل التي قد تحرم مستخدم تقنية المعلومات من الحصول على الخدمات المناسبة المتوقعة، سواء كانت توقفاً لكامل النظام أم عدم قدرة المستخدم على الوصول إلى تطبيق ما لأي سبب من الأسباب الكثيرة جداً، أو عدم نجاح عملية الدخول بسبب خطأ مطبعي في كتابة كلمة المرور ناجم عن مشكلة "زلات الأصابع(*) Fat Fingers" أو أي مشكلة أخرى. ويطلق على المشكلة المُبَلَغ عنها اســم الحادثة، وهي نوع من أنواع الانحراف عن عمليات التشــغيل القياســية. وعلى الرغم من أن العديد من إدارات تشــغيل تقنية المعلومات تمتلك إدارة تســمى مكتب المســاعدة أو مجموعة دعم العملاء، فإن هذه الإدارة العامة يشــار إليها هنا باســم مكتب الخدمــة. فمكتــب الخدمة يكون عادةً هو صاحب عمليــة إدارة الحوادث، على الرغم من أن كل مجموعات دعم الخدمات عبر تقنية المعلومات قد يكون لها دور في إدارة الحوادث.

إن الهــدف من العمليات الفعالة لإدارة الحوادث هو اســتعادة العمليات التشــغيلية الاعتيادية في أسرع وقت ممكن وبطريقة فعالة من حيث التكلفة وبأقل تأثير ممكن، سواء كان التأثــير في الأعمال بكاملها أم في المســتخدمين. ولا ينبغي أن يكون ما تعنيه "السرعة" هنا موضعاً للتأويل أو التفسير، حيث يدعو آيتل إلى تحديد المعايير الخاصة بالإطار الزمني لاســتعادة الخدمات في اتفاقيات مســتوى الخدمة التي تحدثنا عنها في الفصل السابع عشر

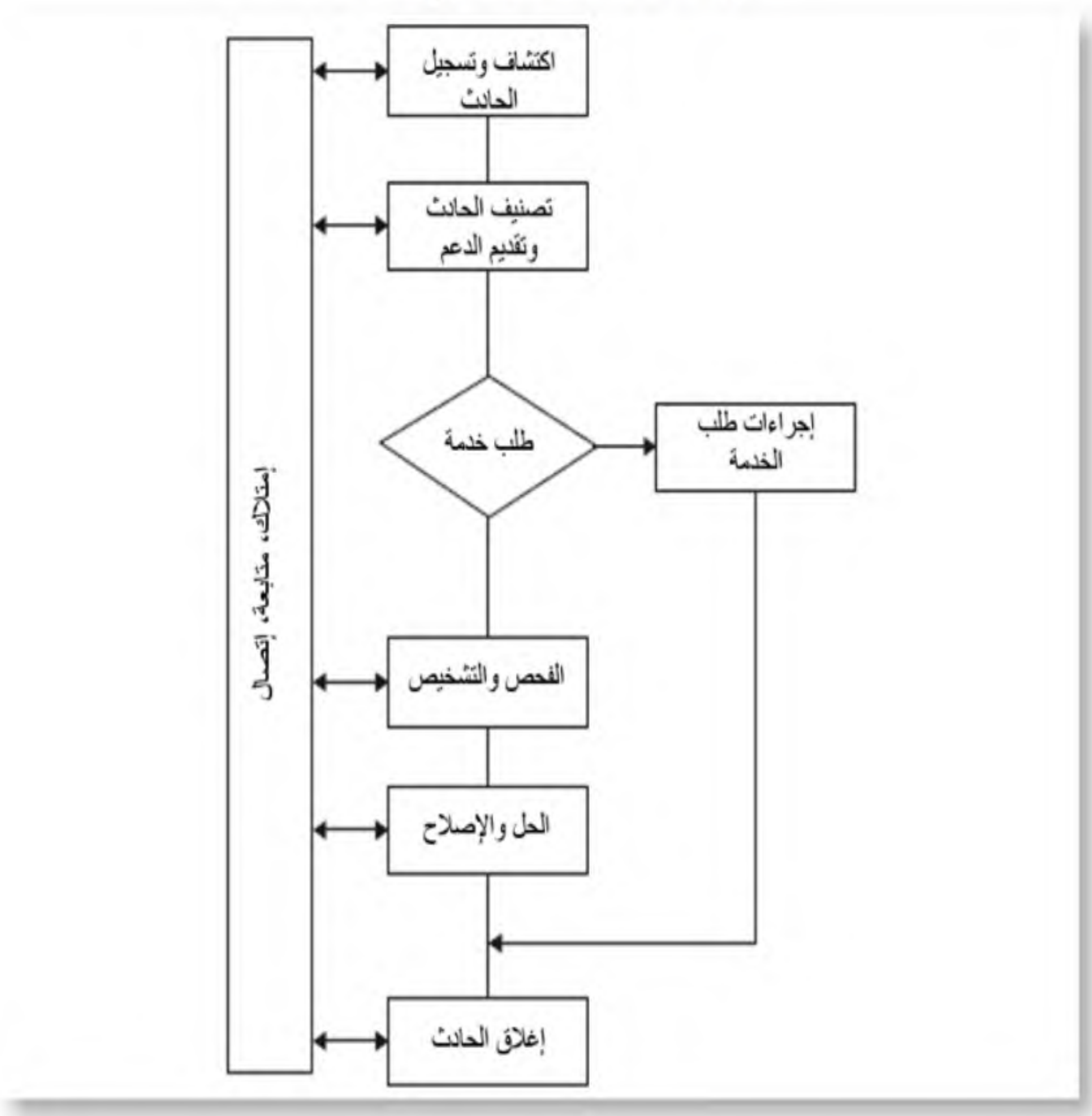
(*) هي مشكلة تقع نتيجة مدخلات خاطئة من خلال لوحة مفاتيح الحاسب الآلي (المترجم).

مــن هذا الكتاب. إن الاتفاقيات الفعالة لمســتوى الخدمــات SLAs هي إحدى المكونات الهامــة في البنية التحتية لتقنية المعلومات، فوجودها مهم بالنســبة للممارســات الخاصة بحوكمــة تقنية المعلومات. فالعنصر الأول في عملية إدارة الحوادث في آيتل هو اكتشــاف الحادثة وتوثيقها من قبل مكتب الخدمة، كونه النقطة الوحيدة للاتصال. ويمكن أن تشمل هذه الحوادث مســائل مثل أن يقوم المســتخدم بالاتصال بســبب وجود مشاكل معينة في التطبيــق أو أن تقوم العمليات التشــغيلية لتقنية المعلومات بإعلام مكتب الخدمة بإحدى المشاكل المتعلقة بمعالجة التطبيق.

بمجرد اســتلام الحادثــة، يجب أن يقوم مكتــب الخدمة بتصنيفها مــن حيث أولويتها priority، وأثرهــا impact، وإلحاحيتها urgency. إذ إن تحديد أولويات للحوادث المبلغ عنها يعد واحداً من أكثر القضايا الهامة في إدارة حوادث تقنية المعلومات. فكل شخص يبلغ عن حادثة يعتقد بأنها الأهم على الإطلاق، لذلك فوحدة إدارة الحوادث لديها مهمة صعبة تتمثل في تحديد الأولوية النســبية للحادث المُبَلَغ عنه وأهميته، وتأثيره في العمل. الشــكل التوضيحــي (٦-٥) يلخص دورة الحياة لأحد حوادث تقنيــة المعلومات ابتداءً من الاتصال الأوليّ وصــولاً إلى الحل والإغلاق. والنقطة الأساســية هنا هي أن نفهم أفضل الممارســات المُوصى بها والخاصة بمكاتب الخدمة وأن نبحث عن الاتفاقيات الرسمية لمستوى الخدمات، عــلى أنها جــزء من عملية إدارة مســتوى الخدمة، وذلك لتحديد أولويــات الحوادث التي تحتاج إلى حل، والجهود المبذولة في حلها، والتعافي من الحوادث. يجب أن تعتمد اتفاقيات مســتوى الخدمة على مدى تأثير أو مدى حساسية الحادث على وحدة الأعمال التي قامت بالتبليغ عنه أو على المؤسســة بأكملها. فيجب على ســبيل المثال أن تقوم إدارة الحوادث بتقدير عدد المســتخدمين المتضررين جراء العطل المبلغ عنــه والخاص بإحدى المعدات أو الأجهزة المادية. وبالطريقة نفسها، فإن الإبلاغ عن مشكلة تتعلق بعملية الإقفال المحاسبي في نهاية الشهر يجب أن تحدد له درجة أهمية أعلى من الإبلاغ عن مشكلة تتعلق بتطبيق يقوم بإصدار أوامر الشراء.

شكل توضيحي (٦-٥)

دورة حياة إدارة الحوادث في الآيتل



أضــف إلى ذلك، أنه ينبغي لفت الانتباه إلى إلحاحية الحادث المبلغ عنه. حيث تشــير الإلحاحيــة إلى السرعــة اللازمة لحــل حادثة لها تأثير معين. ولا يتعــين دائماً حل الحوادث الكبيرة الأثر بشــكل فوري أو افــتراضي. في الغالب يكون الإبلاغ عــن الحوادث التي تفيد بأن مجموعة كبيرة من المستخدمين لا يستطيعون العمل إطلاقاً جراء بعض الانقطاعات في الخدمــات تكون له درجة إلحاحية أكبر من الإبلاغ الذي يقوم به أحد كبار المديرين لطلب

تغيير وظيفة تشغيلية معينة. لذا يجب على فريق إدارة الحوادث التحقيق في الحوادث المبلغ عنها في أقرب وقت ممكن لتحديد مداها وتأثيرها. وربما يدل إخفاق أحد المكونات الذي يتم التبليغ عنه على أن هذا الجهاز خارج الخدمة أو أنه متوقف عن العمل. ويكون هذا النوع غالباً من الحوادث غير معقد كثيراً ونسبياً يمكن إصلاحه بسهولة. في حين قد يكون فشل الاتصالات، الذي ربما يؤثر في العديد من وحدات الأعمال الدولية ومن ثم ربما يؤخر الإقفال المالي الشهري، أكبر بكثير من حيث الحجم والنطاق.

وبمجرد تسجيل الحادث، يجب أن تبدأ عملية التحقيق والتشخيص. فإن لم يتمكن مكتب الخدمة من حل الحادث، فإنه يجب أن يُحيلَه إلى مستويات أخرى من الدعم الفني الخاص بتقنية المعلومات ليقوموا بحلها. وعلى أي حال، ينبغي على جميع الأطراف التي تعمل على الحادث الاحتفاظ بالسجلات المتعلقة بالإجراءات التي يقومون بها، وذلك من خلال التعديل على ملف مشترك خاص بتسجيل الحوادث. إذ يمكن حل بعض الحوادث من خلال عملية الإصلاح السريع التي يقوم بها مكتب الخدمة، والبعض الآخر يكون من خلال قرارات أكثر رسمية، أما في حالة المشاكل الأكثر أهمية، فيكون الحل من خلال اتباع الحلول البديلة لإعادة الأمور إلى نصابها من خلال عملية جزئية والمطالبة بتقديم طلب رسمي Request For Change (RFC) لتغيير النظم أو البائع أو أي شيء نحتاجه إلى إصلاح مثل هذه المشاكل ذات الأهمية الكبيرة. وعند وقوع أي حادث، لا بد من تنظيم الجهود الإصلاحية المبذولة لحل المشكلة وتنسيقها مع وحدة إدارة الحوادث المالكة للمسألة إلى أن يتم إيجاد الحل. ولا بد من الاحتفاظ بالوثائق السليمة للقيام بتتبع الحادث إلى أن يتم حله. وقد يتم إغلاق الحادث رسمياً بمجرد أن يتم إصلاح الأمور. أو إذا لم يحل بسهولة فإن الحادث يجب أن يُمرر إلى الوحدة المختصة بعملية إدارة المشاكل كما سنوضح لاحقاً.

ترتبط جميع عمليات آيتل إلى حد ما بعضها مع بعض، ولكن في العديد من الحالات تمثل إدارة الحوادث خط الدعم الأول بين مستخدمي أو عملاء خدمات تقنية المعلومات وإدارة تقنية المعلومات نفسها. لذا يجب أن تكون إدارة الحوادث أكثر تنظيماً من "مكاتب المساعدة" التي كانت موجودة في السابق عندما كان المستخدمون الذين يقومون بالتبليغ عن المشاكل لا يحصلون في الغالب على المساعدة الكافية والتي ربما لا تتجاوز القيام بإعادة تعيين كلمة

المرور. إن إدارة الحوادث هي نقطة الاتصال الأولى بين العملاء - المستخدمين - وإدارة تقنية المعلومات بشــكل عام. تنشــأ الحوادث، نتيجة الأعطال أو الأخطــاء في البنية التحتية لتقنية المعلومات، والتي تؤدي إلى انحرافات حقيقية أو محتملة في العمليات التشغيلية المخطط لها للخدمات. في بعض الأحيان ربما يكون ســبب وقوع هذه الحوادث واضحاً ويمكن معالجته أو إصلاحــة دون الحاجة إلى مزيد من التحقيقات. وفي حالات أخرى من الممكن أن يكون هناك حاجة لإجراء إصلاحات في المعدات أو البرمجيات. الأمر الذي يســتغرق بعض الوقت لتنفيذه. قــد تكون الحلول قصيرة المدى حلولاً بديلة للحادث، وهي تعد حلاً سريعاً للعودة إلى عملية التشــغيل. أو قد تكون طلب تغيير Request For Change (RFC) رســمياً موجهاً لعملية إدارة التغيــير لإزالة الخطأ. أحــد الأمثلة على الحلول البديلة أو الحلــول القصيرة المدى، هو مطالبة العميل بأن يقوم بإعادة تشــغيل جهاز الحاســب الشخصي أو إعادة ضبط الإعدادات الخاصة بخطوط الإتصالات دون التطرق مباشرة إلى السبب الحقيقي لحدوث المشكلة.

عندما يكون السبب الحقيقي للحادث غير معروف، فإنه يكون من المناسب رفع سجل مشــكلة لخطأ غير معروف في البنية التحتية. ويتم رفع سجل المشكلة فقط في حال كانت عمليات التحقيــق مضمونة ومكفولة، ويكون من الواجب تقييم تأثيرها الفعلي والمحتمل. فنجاح معالجة ســجل المشــكلة ســيؤدي إلى تحديد الخطأ الأســاسي. ويمكن تحويل حالة السجل بعد ذلك إلى خطأ معروف بمجرد إيجاد حل بديل و / أو RFC.

إدارة المشاكل الخاصة بتشغيل الخدمة:

عندما تواجه عملية إدارة الحوادث انحراف نتيجة سبب أو علة غير معروفة، فإنه يجب أن تُمرر تلك الحادثة إلى عملية إدارة المشــاكل في آيتل لحلها. والهدف من ذلك هو تقليل التأثير الكلي للمشاكل من خلال عملية رسمية للكشف والإصلاح، والقيام باتخاذ الإجراءات اللازمــة لمنع تكرارها. إن عملية إدارة المشــاكل هي الخطــوة التالية في مدى أهمية بعض الحوادث المبلغ عنها، وينبغي النظر إلى هذه العملية من حيث ثلاث عمليات فرعية: إدارة مراقبة المشــاكل وإدارة مراقبة الأخطاء والإدارة الرائدة للمشــاكل. يعرف آيتل "المشــكلة Problem" على أنها الســبب الرئيسي غير المعروف ينتج عنــه واحد أو أكثر من الحوادث، ويُعرف "الخطأ المعروف Known Error" على أنه مشكلة قد تم تشخيصها بنجاح وتعريف

الحل البديل لها. ليس ضرورياً أن تكون الفكرة هنا هي إيجاد وحدة إدارية ثانية في إدارة تقنية المعلومات لكي تستقبل الحوادث المبلغ عنها لدى مكتب المساعدة، ولكن الفكرة هي أن يُحدد متى وكيف يجب أن يتم تمرير بعض حوادث مكتب المساعدة المبلغ عنها إلى شخص أو سلطة أخرى لتشخيص المسألة المبلغ عنها بشكل أفضل والتعامل معها على أنها مشكلة. إن العملية الفعالة لإدارة المشكلة يمكنها أن تفعل الكثير لتحسين مجمل الخدمة المقدمة لعملاء تقنية المعلومات.

بالإضافة إلى حل أي حادث فردي يتم إرساله إلى عملية إدارة المشاكل، فإنه ينبغي على تقنية المعلومات أن تسعى لإيجاد عمليات لتحسين التحكم في المشاكل والأخطاء، متضمناً ذلك الحفاظ على البيانات للمساعدة في تحديد الاتجاهات واقتراح إجراءات محسنة للوقاية الاستباقية من المشاكل. لذا لا بد من الاحتفاظ بالمعلومات المتعلقة بالحلول و/أو الحلول البديلة الخاصة بالمشاكل التي تم حلها، بالإضافة إلى سجلات المشاكل المغلقة. في كثير من الحالات، قد تواجه إدارة المشاكل موقفاً يتطلب ضرورة الذهاب إلى خطوة أبعد وتقديم طلب تغيير RFC رسمي، إما من خلال إدارة تطوير تقنية المعلومات وإما من خلال بائع الأجهزة أو البرامج.

وتركز عملية إدارة المشاكل على إيجاد أنماط بين الحوادث والمشاكل والأخطاء المعروفة. إذ إن المراجعة التفصيلية لهذه الأنماط تسمح للمحلل بحل المشكلة عن طريق النظر في العديد من الاحتمالات وتقليصها إلى أن يصل إلى الحل، وهذا ما يسمى بتحليل "السبب الجذري" Root Cause. فهناك العديد من التقنيات الجيدة المستخدمة في حل وتصحيح المشاكل التي تكون غالباً نتيجة مجموعة من العوامل التقنية وغير التقنية. وتعد إدارة المشاكل مجالاً جيداً لتشخيص عمليات تقديم خدمات تقنية المعلومات من أجل تحقيق مستوى فهم أفضل للصحة العامة لعمليات تقنية المعلومات. ويمكن جمع المزيد من المعلومات من خلال فهم عدد طلبات التغيير RFCs التي تم رفعها، ومدى تأثير تلك الطلبات في إتاحة وموثوقية الخدمات كافة المقدمة في تقنية المعلومات، ومقدار الوقت المستغرق في عمل التحقيقات والتشخيص لأنواع مختلفة من المشاكل عن طريق الوحدة التنظيمية أو البائع، وعدد وتأثير الحوادث التي تقع قبل أن يتم حل المشكلة الجذرية أو تأكيد الخطأ المعروف، والخطط من أجل حل المشاكل المفتوحة فيما يتعلق بالأفراد

والاحتياجات الأخرى من الموارد، وكذلك التكاليف ذات الصلة والمبالغ المرصودة في الميزانية.

تعد عمليات إدارة المشـاكل الخاصة بتشـغيل خدمات تقنيـة المعلومات في آيتل من الأمـور الهامة من أجل فهم وتقييم الصحة العامة لعمليات تشـغيل البنية التحتية لتقنية المعلومـات. فالعمليـة الفعالة لإدارة الحوادث تكون ضرورية لاسـتقبال مكالمات العملاء واتخاذ الإجراءات التصحيحية الفورية، في حين أن عملية الإدارة الفعالة للمشاكل قد تذهب خطـوة أبعـد من ذلك حيث تعمل على تحليل وحل المشـكلة من خـلال البدء في تقديم طلبات التغيير RFCs عند الضرورة، وفيما عدا ذلك فإنها تعمل على تحسين رضا العملاء.

حوكمة تقنية المعلومات وأفضل ممارسات تقديم الخدمة في آيتل:

أوجـزت الفقرات السـابقة بعض عمليـات دورة حياة إدارة الخدمـة الأكثر أهمية في آيتل. حيث تقوم إدارة الخدمات في آيتل بوضع الخطوط العريضة لعمليات إطلاق وإدارة وضبط جميع مستويات خدمات تقنية المعلومات مع التأكيد على تحقيق رضا العميل. إن إرشادات آيتل تذهب إلى ما هو أبعد من الرقابة الداخلية، فهي تشمل إدارة تكاليف تقنية المعلومات، ووضع القياسات والمقاييس، وغيرها من قياسات تحسين الجودة.

يدعـو آيتل أي إدارة مـن إدارات تقنية المعلومات إلى أن تقوم ببناء برنامج للتحسـين المسـتمر للخدمات من أجل مراجعة وتحليل وتقديم توصيات بشـأن فرص التحسـين في كل مرحلـة من مراحل دورة حياة تقديم الخدمات في آيتل والتي تمت مناقشـتها في هذه الأقسـام. إن عمليات دورة حياة إدارة الخدمة في آيتل قد تم اعتمادها بشـكل متزايد من خلال إدارات تقنية المعلومات في جميع أنحاء العالم. إذ إن التركيز على الخدمة يرفع أهمية مـوارد تقنية المعلومات والبنية التحتية الداعمة لها بالنسـبة للمؤسسـة بكاملها وعملائها وأصحاب المصلحة فيها.

إن دورة حيـاة إدارة الخدمـة في آيتل عباره عن سلسـلة من العمليـات المترابطة لأفضل الممارسـات التي تدعم إدارة البنية التحتية لتقنية المعلومات وإدارة المؤسسـة. إن تطبيقات تقنية المعلومات تقع في وسـط هذه المعضلة وتمثل منطقة مركزية رئيسية لاهتمامات الرقابة الداخليـة وحوكمة تقنية المعلومات. وفي حين أن عمليات إدارة المشـاكل والحوادث والتغيير

في آيتـــل ، من بين أمور أخرى، تميل إلى الدعوة إلى إنشـــاء إدارة كبـــيرة جداً لتقنية المعلومات بمســـتويات متعددة من المـــوارد البشرية والإدارية. فإنه يمكن أيضاً تطبيق هذه الممارســـات المثـــلى الموجـــودة في آيتل على مؤسســـة أصغر من ذلك بكثير. حيث يمكـــن تطبيق آيتل على جميـــع إدارات تقنيـــة المعلومات بمختلف أحجامها! وحتى تكون المؤسســـة متوافقة مع آيتل ، فانهـــا لا تحتاج إلى مســـتويات متعددة من موظفي الدعم، بـــل تحتاج إلى النظر في مختلف عمليـــات دعـــم وتقديم الخدمات من منظور أفضل الممارســـات في آيتل. قـــد لا تحتاج إدارة صغيرة لتقنية المعلومات إلى إنشاء إدارات منفصلة لإدارة الحوادث وإدارة المشاكل مثلاً. ولكن يجب أن ننظر في كل منها على أنها عمليات منفصلة مع إجراءات رقابية فريدة ومميزة. حتى وإن كانت إدارات تقنية المعلومات في المؤسســـة صغيرة جداً، فإنها ينبغي أن تُعَامِل كل مجال من مجالات العمليات الموجودة في آيتل على أنه مجال مستقل من أجل تحسين العمليات.

تعد البنية التحتية لتقنية المعلومات أحد المجالات الهامة لحوكمة تقنية المعلومات. في كثير من الأحيان، قد ركز كبار مديري تقنية المعلومات وغيرهم من كبار المديرين اهتمامهم عـــلى الضوابط الخاصة بالتطبيقات والضوابط العامة لتقنية المعلومات التي كانت موجودة في الماضي. أما في عالم اليوم الذي يتسم بالعمليات المعقدة التي تدعم البنية التحتية لتقنية المعلومات، فإن عمليـــات آيتل المبينة في هذا الفصل تصف بعض المجالات الممتازة للعناية بحوكمة تقنية المعلومات.

ملاحظة

١- كتـــب الآيتل متاحة من خلال مكتب المملكة المتحدة والذي يســـمى مكتب المكتبة (TSO)، والذي يمكن العثور عليه في الموقع www.tsoshop.co.uk.

الفصل السابع

معايير حوكمة تقنية المعلومات: أيزو ٩٠٠١ و٢٧٠٠٢ و٣٨٥٠٠

في الأعـوام التي تلت الحرب العالميـة الثانية، برزت الولايات المتحـدة زعيماً اقتصادياً وسياسـياً عالمياً. وبسـبب هذه الهيمنة، فقد تجاهل الكثيرون في الولايات المتحدة المعايير المتعلقة بأفضل الممارسـات التجاريـة التي تم تطويرها واسـتخدامها في أماكن أخرى من اقتصادنا العالمي المترابط. إن هذه المعايير الدولية لأفضل الممارسات هي نتاج جهود تعاونية تأخذ بعين الاعتبار مجموعة واسعة من الاحتياجات والمتطلبات المحلية. إن مصدر العديد من هـذه المعايير هو منظمة المقاييس والمواصفات الدوليـة International Standards Organization (ISO;www.iso.org) وهـي هيئة يقع مقرها في جنيف بسـويسرا، وقد قامت بإصدار المعايير المعتمدة والمتعارف عليها والتي تغطي مجموعة واسعة من المجالات بدءاً من المواصفات الخاصة بأسـنان التثبيت الملولبة المسـتخدمة في محركات السـيارات إلى سـمك بطاقة الائتمان الشـخصية ووصولاً إلى معايير الجودة الخاصة بتقنية المعلومات. وقد تم توسـيع هذه المعايير على مر السنين لتشمل العديد من المجالات التي تعتبر مهمة بالنسبة لحوكمة وجودة المؤسسات.

لا بد أن يتمتع كبار المديرين التنفيذيين بمسـتوى فهم معين لأدوار معايير الأيزو وأيّ منها تناسـب مؤسسـاتهم، كما يجب عليهم فهم المعايير الهامة بالنسـبة لحوكمة فعالة لتقنية المعلومات. ويستعرض هذا الفصل ثلاثة من هذه المعايير التي تعتبر مهمة بالنسبة للممارسـات الفعالة لحوكمة تقنية المعلومات. وبعد مناقشة بعض المعلومات الأساسية عن كيفية تطوير تلك المعايير الخاصة بأيزو وسـبب أهميتها، فإننا سنقوم بتسليط الضوء أولاً عـلى المعيار العالمي الذي يطلق عليه اسـم أيـزو ٩٠٠١ (ISO 9001)، وعلى الرغم مـن عدم تركيز هذا المعيار على قضايا حوكمة تقنية المعلومات على وجه الخصوص، فإن المبادئ التي جاءت في هذا المعيار قد شجعت العديد من المؤسسات على الصعيد العالمي على وضع وتنفيذ الممارسـات الخاصة بجـودة الإنتاج والعمليات التجارية الأخرى بصورة مستمرة.

وعــلى الرغم من وجود مجموعــة كبيرة من معايير الأيزو التي قــد يمكن تطبيقها على حوكمة تقنية المعلومات، فإن هذا الفصل ســيقوم باســتعراض اثنين من تلك المعايير وبيان أهميتهــا وهما: أيــزو ٢٧٠٠٢ (ISO 27002) وأيــزو ٣٨٥٠٠ (ISO 38500). واســتكمالاً لحديثنــا عن اتفاقيات مســتوى الخدمــة SLAs التي تم تقديمها في الفصل الســابع عشر مــن هذا الكتاب، فــإن هذه المعايير تعمل عــلى توضيح إطار العمل من أعلى إلى أســفل للقيام بتحديد ملامح عمليات إدارة الخدمات الضرورية لتقديم خدمات عالية الجودة. قد يكون فهم المعايير المناسبة لمنظمة الأيزو ISO أمراً هاماً بالنسبة لبعض الممارسات الخاصة بحوكمــة تقنية المعلومات. فعلى الرغم من أن هذه المعايــير يتم تطبيقها غالباً من خلال إدارة الجودة أو إحدى الإدارات بالمؤسســة، فإنه يتوجب عــلى المدير الأول أن يكون ملماً بأهمية تلك المعايير ومجمل عمليات الأيزو.

معلومات أساسية عن معايير الأيزو:

قد يكون (مصطلح الأيزو) مربكاً بعض الشيء بالنســبة للبعض، فهو يشــير إلى منظمة المقاييس والمواصفات الدوليــة International Standards Organization. وهي عبارة عن هيئة متخصصة في وضع المعايير العالمية، يقع مقرها في مدينة جنيف بســويسرا. وهي الجهة المســؤولة عن تطوير ونشر مجموعة واسعة من المعايير الدولية التي تتعلق بالعديد مــن مجالات وإجراءات الأعمال. بعض معايــير الأيزو يعتبر عاماً جداً كالمعيار أيزو ١٤٠٠١ (ISO 14001) ، وهــو المعيار الذي يحدد المتطلبات الخاصة بالنظم الفعالة للإدارة البيئية، في حــين يكون البعض الآخر منها مفصلاً ودقيقاً، كالمعيــار الذي يتناول المواصفات الخاصة بحجم وســمك بطاقات الائتمان البلاســتيكية. تعود أهمية المعايير الواسعة للأيزو إلى أنها تســمح لجميع المؤسسات على مستوى العالم باســتخدام اللغة نفسها، وذلك عندما تصرح تلك المؤسســات بأن لديها المعيار نفســه، وليكن على ســبيل المثال، معيــار النظام الفعال لــلإدارة البيئية أيــزو 14001. كما أن هناك العديد من المعايــير الأكثر تفصيلاً والتي تعتبر هامة وحساسة للغاية، مثل تلك الخاصة بماكينة الصراف الآلي والموجودة في كل أنحاء العالم والتي تتوقع أن تستقبل جميعها بطاقات ائتمان لها الحجم والسُمْك نفسهما.

يتــم تطوير معايير الأيزو من خــلال تضافر جهود العديد من المنظمات الوطنية المعنية بوضع المعايــير، مثل المعهد الأمريكي للمعايير الوطنية American National Standards Institute، أو غــيره مــن المجموعات المنتــشرة في جميع أنحاء العالم. تبــدأ عملية وضع المعايير بشــكل عام بضرورة معروفة تُحتِّم وجود معيار في مجال ما. مثال على ذلك معيار أيــزو ٢٧٠٠١ (ISO 27001) والــذي يقوم بتحديد متطلبات رفيعة المســتوى لنظام فعال لإدارة أمــن المعلومات. وقد تم تطوير هــذا المعيار من خلال جهود اللجان الفنية الدولية التــي ترعاها منظمة الأيــزو بالتعاون مع اللجنــة الدولية الكهروتقنيــة International Electrotechnical Commission، وهي إحدى الهيئات المعنية بوضع المعايير الدولية. لا يحتــوي هذا المعيار على أية متطلبات تفصيلية، لكنه يحتوي على عبارات رفيعة المســتوى على غرار ذكر "يجب على المؤسسة". في بعض المجالات، يتم وضع هذا النوع من الإرشادات في الإجراءات المتعلقة بعملية تدقيق تقنية المعلومات التي تم الحديث عنها في العديد من فصول هذا الكتاب.

ونظراً لمشــاركة العديد من الهيئــات الحكومية الدولية والمجموعــات المهنية والخبراء المستقلين في عملية وضع معايير الأيزو، فإن عملية بناء واعتماد أي وثيقة من وثائق منظمة الأيــزو تحتاج غالباً إلى وقت طويل. حيث تقوم لجنة من الخبراء بتطوير مســودة مبدئية للمعيار الذي يغطي مجالاً ما، بعد ذلك يتم إرســال تلك المســودة للمراجعة وإبداء الرأي قبــل تاريخ محــدد، ثم تقوم اللجنــة في النهاية بمراجعة التعليقات على المســودة قبل أن تقوم بإصدار المعيار الجديد أو إرســال مســودة منقحة لإجراء جولة أخرى من المراجعات والتغييرات المقترحة. ويتم نشر معيار الأيزو عادة بعد مروره بالعديد من المراحل التي يتم من خلالها إعداد المســودات والنظر في التعليقات الخاصة بها. يمكن للمؤسسات بعد ذلك أن تقــوم باتخــاذ الخطوات اللازمة للامتثال لهذا المعيار. ويجب على المؤسســة أن تتعاقد مــع مدقق خارجي معتمد يمتلك مهارات في هذا المعيار ليقوم بالتصديق على امتثالها لهذا المعيار.

وقد شــاركت العديد من المؤسسات الأمريكية للمرة الأولى في هذه المعايير الدولية من خــلال إطلاق معايير أيــزو ٩٠٠٠ (ISO 9000) الخاصة بنظــام إدارة الجودة في ثمانينيات

القرن الماضي، وسـيتم مناقشة هذا المعيار لاحقاً في هذا الفصل. كانت الشركات الأمريكية تواجة مشـاكل تنافسية بالنسبة للمنتجات التي تخضع لمعايير تصميم عالية الجودة والتي كانت مطبقة في المنتجات غير الأمريكية في ذلك الوقت مثل السيارات اليابانية. فقد قامت المؤسسـات اليابانية بتصميم العديد من المنتجات العالية الجودة من خلال اتباع ما أصبح يعـرف بأيزو ٩٠٠٠ (ISO 9000)، وبدأ المصنعـون في الولايات المتحدة بتعديل العمليات الخاصة بهم للامتثال لهذه المعايير الخاصة بالمنتجات ذات الجودة العالية. وقد سمح هذا الامتثال بمعيار أيزو ٩٠٠٠ (ISO 9000) للمؤسسات في جميع أنحاء العالم بتصميم عملياتها التشغيلية وفقاً لمعيار واحد ثابت، ومن ثم التأكيد على أن لديهم نظاماً مُفَعَلاً ومعمولاً به لإدارة الجودة وفقاً للمعيار الدولي.

تعد معايير الأيزو أكثر تحديداً وضبطاً من الإرشـادات الخاصة بأفضل الممارسات لمكتبة البنية التحتية لتقنية المعلومات (آيتل) والتي تناولنا الحديث عنها في الفصل السـادس من هذا الكتاب. إذ يتم نشر وضبط هذه المعايير بواسـطة منظمة الأيزو التي تقع في جنيف، والتـي تتبع قوانين صارمة في حقوق التأليـف والنشر. فالمواد الخاصة بها لا يمكن تحميلها مـن خـلال عمليات البحث الاعتياديـة على الإنترنت؛ بل لابد من شرائهـا. إن العديد من معايير الأيزو الفعلية عبارة عن توضيحات تفصيلية للغاية للممارسات التي يجب اتباعها.

تكون الإرشـادات واضحة ولا لبس فيها ولا غموض و تشـير غالباً إلى أقسـام أخرى من هذا المعيار لاتباعها. تستطيع المؤسسة أن تقوم باتباع معايير منظمة الأيزو ISO والاعتماد عليها، وذلك على غرار اتباعها لأفضل الممارسـات الخاصـة بآيتل ، إلا أن عدد معايير الأيزو أكـثر بكثـير من أفضل الممارسـات المُوصى بها في آيتـل. فهي تمثل مقاييس أداء بالنسـبة للمؤسسة مع نظيراتها. فمن خلال الالتزام والتمسك بتلك المعايير العالمية، يمكن للمؤسسة التحقق من أنها تعمل وفقاً لمعيار دولي ثابت، فمعايير أيزو ١٣٤٨٥ (ISO 13485) الخاصة بالمتطلبـات التنظيمية لإدارة الجودة الخاصة بالأجهزة الطبية تقدم مثالاً على ذلك. حيث يحدد هذا المعيار متطلبات الجودة الخاصة بأجهزة الرعاية الصحية للإنسـان، ومن الأمور الأخرى التي يتضمنها هذا المعيار، أنه يدعو المؤسسة التي تقوم بصنع مثل هذه الأجهزة إلى أن تقوم بوضع ضوابط المعايرة المناسبة. ونظراً لتنوع أساليب المعايرة، فإن المعيار لا يمكن

أن يحدد أسـلوباً واحداً فحسـب؛ فهو في جميع الأحوال يشـترط على المؤسسات أن يكون لديها الآليات المناسبة المعمول بها.

ومن الأمور الهامة بالنسـبة للمؤسسـة أن تقوم بقراءة معيار الأيـزو وتعديل عملياتها للتوافق معه؛ ومن الأمور الجيدة أيضاً بالنسـبة للمؤسسـة أن تثبت للآخرين أنها تتبع هذا المعيار. إن شهادة الأيزو هذه عبارة عن عملية مشابهة لعملية التدقيق الخارجي للسجلات الماليـة التي يقوم بها المحاسـبون القانونيـون (CPAs). فعمليات تدقيـق القوائم المالية تتطلـب وجود محاسـب قانوني معتمد يعمـل مدققاً خارجياً معتمـداً لتقييم ما إذا كانت تلك التقارير المالية للمنشأة "معلنة بوضوح" وتَتَّبِع ضوابط داخلية جيدة ومعايير محاسبية معتمدة ومتعارفاً عليها أم لا. فهي تعد مفردات رفيعة المستوى، إلا أن تقريراً كهذا للتدقيق الخارجي الذي يتم التوقيع عليه مع النتائج النهائية المبلغ عنها من شـأنه أن يوفر مسـتوى للتأكيد على أن التقارير المالية نزيهة وتستند إلى إجراءات جيدة للرقابة الداخلية.

إن عملية الحصول على شـهادة الأيزو تشـبه أيضاً عملية التدقيق المالي التي يقوم بها المحاسب القانوني المعتمد والذي يعتمد على التوافق مع معايير التدقيق المقبولة قبولاً عاماً (GAAS) والتـي تقوم بها شركات المحاسـبة العامة الكبرى. وعـلى الرغم من عدم وجود الـشركات "الأربعة الكبار Big4" هنا ، أي مجموعة من الشركات الكبرى لتدقيق الأيزو، فإن منظمات وضـع المعايير تؤهل المراجعين الخارجيين لأداء المراجعـة الخارجية لمعايير الأيزو المختلفـة. حيث لا يوجد للأيزو معايير تدقيق متعـارف عليها GAAS ولكن هناك درجة كبـيرة من التنوع في أهداف التدقيق، فمُرَاجِـع معيار أيزو ٢٧٠٠١ (ISO 27001) الخاصة بنظم إدارة أمن المعلومات سيقوم بالبحث عن الإجراءات الرقابية المختلفة، وهذا مغاير لما سـيبحث عنه مراجع معيار أيزو ١٣٤٨٥ (ISO 13485) الخاصة بنظم إدارة جودة الأجهزة الطبيـة. في جميع الأحـوال، فإن المدقق الخارجي المؤهل لتدقيـق معايير الأيزو قد يحدد الأجـزاء التي تحتاج إلى إجراءات تصحيحية ويقوم بإصدار تقرير للإدارة مشـابه لعمليات التدقيق الداخلي، كما سـيتم مناقشـته في الفصل التاسع عشر من هذا الكتاب. وبمجرد أن يتم تصحيح توصيات مدقق الأيزو، فإن المراجع الخارجي سوف يشهد بأن المؤسسة متوافقة مع المعيار.

وبمجرد اعتماد المؤسسة، فإنها تستطيع أن تعلن للعالم الخارجي أن العمليات المتبعة لديها تُلبي ذلك المعيار الخاص بالأيزو. على سبيل المثال، فإن أحد الزبائن الذين يتعاملون مع أجهزة التشخيص الطبي يريد أن يعرف ما إذا كان المُوَرِد المحتمل متوافقاً مع معيار أيزو ١٣٤٨٥ (ISO 13485) أم لا. وإن هذا المُصَنع للجهاز الطبي نفسه سيرغب أيضاً في الحصول على ضمانات بأن موردي المكونات الأولية لها مؤهلون من قبل الأيزو. وعلى الرغم من وجود مجموعة كبيرة من معايير الأيزو، فإن الأقسام التالية تستعرض عدداً من المعايير التي لها أهمية بالنسبة للضوابط الداخلية والحوكمة والتي تشهد نمواً متزايداً على مستوى العالم في الوقت الراهن.

معايير الأيزو ٩٠٠٠ لإدارة الجودة:

تمتلك معايير الأيزو ٩٠٠٠ (ISO 9000) تراثاً يعود تاريخه إلى أيام الحرب العالمية الثانية. وذلك عندما كان طرفا الصراع بحاجة إلى توحيد قوي لمواصفات المنتجات أثناء القيام بإنتاج العديد منها. حتى وإن كانت هذه المنتجات عبارة عن الرصاص والقنابل، كان يجب عليهم العمل بشكل صحيح لتوحيدها. فقد كانت هناك حاجة لفرض رقابة صارمة على جودة المنتجات. وظهرت بعض الإجراءات القياسية القوية من جانب الحلفاء الغربيين لضمان الجودة، كما ظهرت مهن كالمهندسين الصناعيين وأخصائين للعمل في مراقبة جودة الإنتاج. وبعد انتهاء الحرب، تم إنشاء منظمة الأيزو على أنها جزء من الاتفاقية العامة للتجارة والتعريفات الجمركية General Agreement on Trade and Tariffs (GATT) أو ما يعرف باسم (اتفاقية الجات). وهي إحدى الاتفاقيات الدولية الهادفة إلى جعل العالم يعيش في بيئة أكثر أمناً. كانت معايير الأيزو ٩٠٠٠ الخاصة بنظم إدارة الجودة واحدة من المعايير الأولى التي أصدرتها منظمة الأيزو. وقد لاقت الاهتمام الأول بها والأكبر من قبل البلدان الأوروبية التي كانت تتعافى حديثاً من آثار الحرب.

وقد كانت اليابان واحدة من البلدان التي بحاجة إلى إعادة الإعمار والتعافي من الحروب، وهي البلد التي قامت بتبني نظم إدارة الجودة بشدة في تلك الفترة. وقد قام اليابانيون في خمسينيات وستينيات القرن الماضي بتوجيه دعوة لعدد من خبراء أنظمة الجودة الأمريكيين مثل دبليو إدواردز ديمينج[1] W. Edwards Deming، وآخرين ليقوموا بمد يد العون

والمســاعدة لهم في العديد مــن المصانع اليابانية. وفي الوقت الــذي تم فيه تجاهل هؤلاء الخبراء إلى حد ما في الولايات المتحدة، قامت الصناعة اليابانية بتبني فلســفتهم وتقنياتهم بشــكل كبــير وملحوظ. وبحلول منتصف الســبعينيات من القرن المــاضي بدأت الشركات اليابانية المصنعة للإلكترونيات والســيارات تشــق طريقها بشــكل كبير في أسواق الولايات المتحــدة نظراً لجودة وقيمة منتجاتها. وقــد بدأ الكثيرون في الولايات المتحدة في إدراك أن هذه المنتجات اليابانية الصنع قد تفوقت على منتجاتهم في كثير من النواحي. فقد أصبحت معايير الجودة الخاصة بالأيزو (ISO 9000) عاملاً ذا أهمية متزايدة في قياس وتقييم جودة المنتجات في جميع أنحاء العالم.

إن الأيــزو ٩٠٠٠ (ISO 9000) هــي عبــارة عن عائلة من المعايــير الخاصة بنظم إدارة الجــودة والتــي يتم تنظيمهــا وصياغتها من قبل منظمــة الأيزو. وتتضمــن هذه المعايير متطلبات لأمور مثل:

- مراقبة العمليات لضمان أنها فعالة.
- حفظ سجلات وافية عن إجراءات العمل.
- فحص مخرجات الإنتاج من أجل اكتشاف العيوب، مع بدء الإجراءات التصحيحية المناسبة عند الضرورة.
- مراجعة منتظمة للعمليات الفردية ونظام الجودة الشاملة من أجل الفاعلية.
- تسهيل عمليات التحسين المستمر.

يشــير كل بند من هذه البنود إلى مجموعة من العمليات، لا إلى إجراءات معينة. ولكي تثبت مؤسســة ما أنها متوافقة على ســبيل المثــال مع الأيزو ٩٠٠٠ (بالتحديــد معيار أيزو ٩٠٠١) - والذي يقوم بمتابعة العمليات الرئيســية لتكون أكثر فاعلية، فإنه يتوجب عليها في كثير من الأحيان أن تقوم بعمل العديد من التغييرات في إجراءاتها الإدارية ووثائقها الداعمة. إن الامتثال بأحد معايير الأيزو يخلق أيضاً مســتوى مطلوبــاً من التوقعات. فعندما تحصل المؤسســة في أي مــكان في العالم على مثل هذه المعايير، فهي بذلــك تعلن أنها تمتلك أنظمة فعالة ومعمولاً بها لإدارة الجودة. إن المؤسســة التي يتم تدقيقها واعتمادها بشكل مستقل

لتكون متوافقة مع أيزو ٩٠٠١ على سبيل المثال، قد تعلن صراحة أنها "معتمدة من الأيزو ٩٠٠١" أو "مسجلة لدى الأيزو ٩٠٠١". لا تضمن شهادة معيار أيزو ٩٠٠١ الامتثال (ومن ثم الجودة) للمنتجات والخدمات النهائية، وإنما هي فقط شهادة تدل على أنه يتم تطبيق العمليات التجارية والإنتاجية الملائمة.

تتم عملية الاعتماد الفعلية من خلال الفحص الذي يقوم به أحد المدققين المعتمدين في الأيزو والمتخصصين في معيار محدد من معاييرها. وكما تحدثنا سابقاً فان هذه العملية تشبه عملية المراجعة والتدقيق التي يقوم بها المحاسبون القانونيون(CPA's) لاعتماد القوائم المالية الخاصة بإحدى المؤسسات. وبالتنسيق مع منظمات المعايير الوطنية لديهم يتم التفويض والسماح لمدققي الأيزو بتسجيل امتثال المؤسسة لمعيار فريد من معايير الأيزو.

إن معايير الأيزو ٩٠٠٠ وغيرها من المعايير الأخرى للأيزو تفرض على المؤسسة متطلبات توثيقية ضخمة، فلا يكفي أن تدعي المؤسسة بأنها قامت بتوثيق عملية ما لمرة واحدة فقط. بل يجب أن تكون هناك عملية مستمرة لإبقاء هذا التوثيق فعالاً ومستمراً. في السنوات الماضية، بذلت العديد من المؤسسات الجهود لتوثيق إحدى المبادرات أو العمليات الجديدة للمرة الأولى ولكنها فشلت في المحافظة على هذا التوثيق. وقد تعرض العديد من مدققي تقنية المعلومات لمثل هذه الحالات. فكثيراً ما كانوا يسألون عما إذا كان قد تم توثيق النظام أو العملية التي هم بصدد مراجعتها حالياً، وفي حال كانت الوثائق غير محدثة أو غير موجودة، فإن هذا القصور سيظهر غالباً في نتائج التقرير الخاص بعملية التدقيق، وفي كثير من الأحيان لا يؤدي ذلك إلا إلى القليل من الإجراءات التصحيحية النهائية. إن الامتثال لمعايير الأيزو ٩٠٠٠ يرفع سقف المتطلبات الخاصة بعمليات الجودة إلى مستوى جديد كلياً. لذا يجب على مراجع الأيزو أن يصدق أو يشهد على امتثال المؤسسة بالمعيار لكي تتمكن من الإعلان للعالم الخارجي بأنها متوافقة مع معيار الأيزو.

إن الأيزو ٩٠٠٠ هو عبارة عن مجموعة من المعايير الخاصة بنظام الجودة القائم على التحسين المستمر، سواء كان ذلك لإحدى المنتجات الصناعية أم العمليات الخدماتية. يوضح الشكل التوضيحي (٧-١) تلك العملية الخاصة بنظام إدارة الجودة التي تقودها سلسلة من الإجراءات الداخلية للتحسينات المستمرة وطلبات العملاء أيضاً. في هذه العملية المستمرة،

يجب مراقبة العمليات الموجودة والإجراءات المخطط لها لإدخال التحسينات وعناصر الإجراءات التي يتم تنفيذها لعمليات المراقبة، وإدخال المزيد من التحسينات المستقبلية. لا تعد عملية التحسين المستمر للجودة من العمليات الجديدة بالنسبة للعديد من كبار المديرين. فقد قام محترفو تطوير نظم تقنية المعلومات بالأساس باستخدام المجموعة نفسها من العمليات العامة التي كانت موجودة منذ الأيام الأولى لتطوير النظم التقنية في عملية تطوير النظم الجديدة في تقنية المعلومات والتي تدعى دورة حياة تطوير النظم SDLC. وقد دعت تلك التطبيقات التي تم تطويرها باستخدام أسلوب عملية دورة حياة تطوير النظم SDLC إلى قدر كبير من الوثائق التي كانت في أغلب الأحيان غير جاهزة. أما اليوم فيتم تطوير تطبيقات تقنية المعلومات من خلال عمليات غير رسمية ودورية وسريعة بشكل أكبر لتطوير التطبيقات.

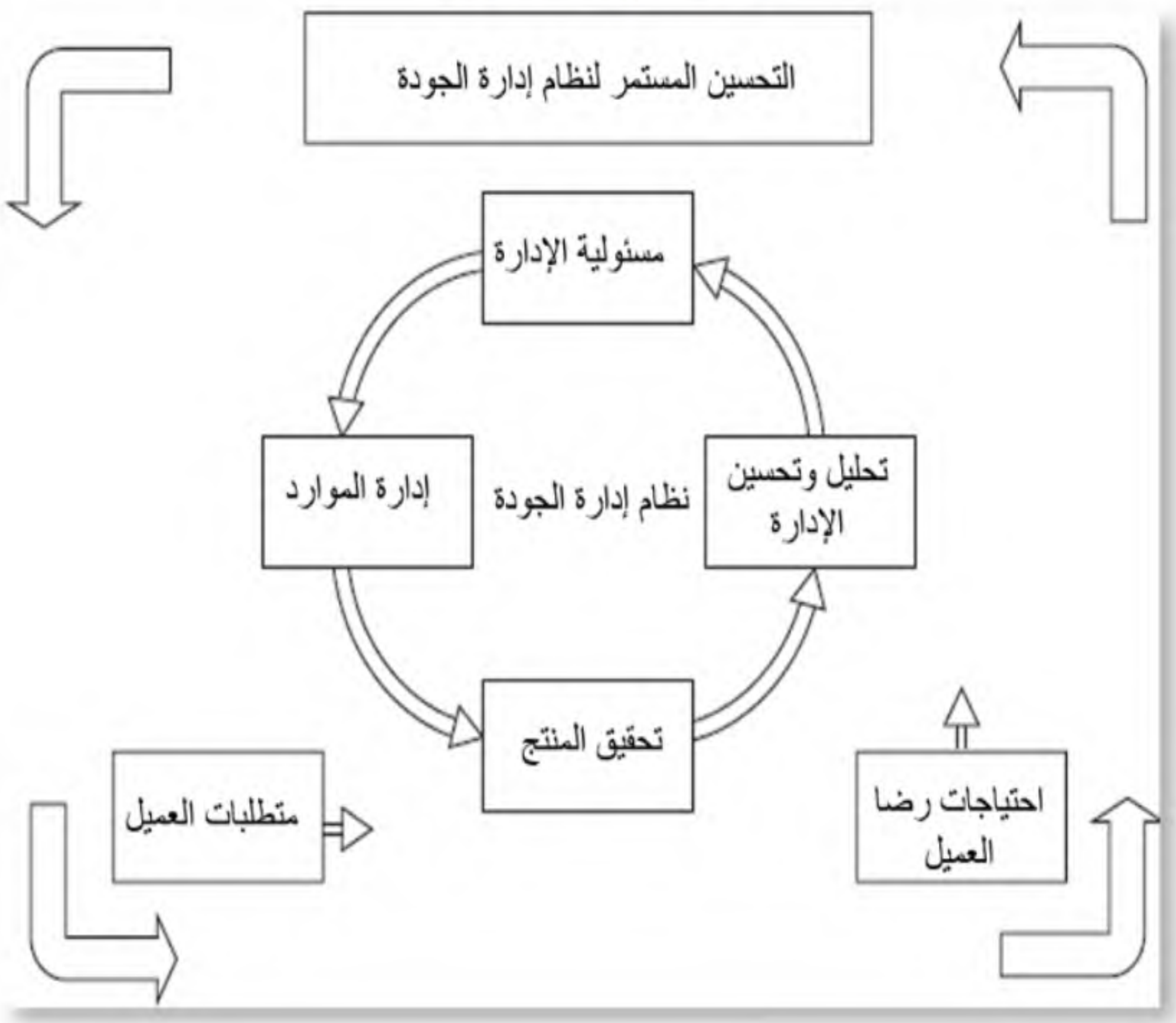
إن التوثيق الصارم والدقيق مهم جداً بالنسبة للمؤسسة التي تسعى للتسجيل في الأيزو، وهو مطلب عالمي. حيث تدعو أفضل الممارسات في الأيزو إلى اتباع التسلسل الهرمي للتوثيق في أي مجال، بدءاً من الإرشادات الرفيعة المستوى التي توضح أسباب الممارسة، وصولاً إلى التعليمات التفصيلية التي توضح الكيفيات التي تتم من خلالها الممارسة. الشكل التوضيحي (٧-٢) يعرض هذا التسلسل الهرمي للتوثيق حيث تم وضع "النماذج والوثائق" في الجزء السفلي من المثلث، والتي تعمل على توفير الأدلة والبراهين. فهذا التوثيق ضروري وأساسي لدعم نظام إدارة الجودة، ومن المؤكد أنه يُطلب من قِبل مدققي التصديق الخارجين للأيزو.

لقد وفر هذا القسم وصفاً رفيع المستوى جداً لمعايير الأيزو ٩٠٠٠ الخاصة بعملية إدارة الجودة. ومع ذلك، قد يتساءل القارئ: "لماذا يجب عليّ الاهتمام بالأيزو، وما الذي لديها لتقدمه لحوكمة تقنية المعلومات؟" نقول، إن التوافق مع هذه العمليات الخاصة بالأيزو ٩٠٠٠ مهم بالنسبة لجميع أنواع المؤسسات لتعلن للإدارة الداخلية الخاصة بها وللعالم الخارجي بأنها تركز على الجودة. ومثال على ذلك، في عام ١٩٩٥ أصبح المعهد الأمريكي للمحاسبين القانونيين أول منظمة مهنية عالمية كبرى معتمدة وحاصلة على شهادة الأيزو ٩٠٠١[٢]. فمن الواجب أن تقوم جميع المنظمات على مختلف المستويات

بالنظــر في تبني عمليات الأيــزو ٩٠٠٠. فكثير من الإعلانات الموجــودة اليوم لكثير من المنتجــات أو الخدمــات المعروضة تصرح أو تذكر أن البائع حاصل على شــهادة الجودة ومعتمد من قبل منظمة الأيزو، ويســتطيع أي عميل طلــب المزيد من المعلومات التي تتعلق بمستوى هذه الشهادة قبل أن يقرر إتمام عملية الشراء.

شكل توضيحي (٧-١)

عملية نظام إدارة الجودة



تحدد معايير الأيزو بعض أفضل الممارســات الرفيعــة في العديد من مجالات العمليات التشــغيلية لتقنية المعلومات. حتى وإن كانت المؤسســة لا تســير بنســبة مئة في المئة في اســتكمال جميع المتطلبات الخاصة بأحد معايير الأيــزو وتكمل متطلبات التدقيق الخاصة بالأيزو، فإن المعايير سوف توفر بعض الإرشادات القوية والمثبتة لبناء عمليات داخلية قوية.

تناقش الأقسـام التالية بمزيد من التفصيـل المتطلبات الخاصة باثنين من هذه المعايير التي تعتبر مهمة بالنسبة للعمليات الفعالة لحوكمة تقنية المعلومات.

شكل توضيحي (٧-٢)

هرمية الوثائق في الأيزو



معايير الأيزو الخاصة بأمن تقنية المعلومات: أيزو ٢٧٠٠٢ و ٢٧٠٠١:

إن أيـزو ٢٧٠٠٢ (ISO 27002) هـو عبارة عن معيار هام في النواحـي الأمنية المرتبطة بتقنية المعلومات، ومصمم لمسـاعدة أي مؤسسـة تحتاج إلى وضع برنامج شامل لإدارة أمن المعلومات أو تحسـين ممارسـاتها الحالية المتعلقة بأمن المعلومات. وبعيداً عن موضوعات الحوكمة وأمن تقنية المعلومات التي نُوقشـت في الفصـل العاشر من هذا الكتاب، فإن أيزو ٢٧٠٠٢ يعـد أحد المعايير التي تخص طائفـة عريضة من مصادر المعلومات وأمن المعلومات بشكل عام. ولأن هناك العديد من الأشكال التي يمكن أن تتواجد بها مثل هذه البيانات، فإن المعيار يأخذ نهجاً موسعاً ويحتوي على مجموعة كبيرة من المعايير الأمنية التي تتعلق بالتالي:

• الملفات الإلكترونية للبيانات والبرمجيات.

• جميع أشكال المستندات الورقية، متضمناً ذلك المواد المطبوعة والملاحظات المكتوبة بخط اليد والصور.

• تسجيلات الفيديو والتسجيلات الصوتية.

• المحادثات الهاتفية وكذلك البريد الإلكتروني والفاكس والفيديو وغيرها من أشكال الرسائل.

الفكرة هنا هي أن المعلومات بجميع أشـكالها لهـا قيمة وبحاجة إلى حماية، تماماً كأي أصل من الأصول الأخرى الموجودة في الشركة. إن العديد من المؤسسات اليوم لا تضع حتى تلك المعايير الأمنية في الحسـبان فيما يتعلق بتلك المجالات الواسعة، لكن معيار أيزو يشير إلى أنه لا بد من تضمين هذه المعايير الأمنية قدر المستطاع. كما يقترح أيضاً ضرورة حماية البنية التحتية التي تدعم هذه المعلومات، والتي تتضمن الشـبكات والنظم والوظائف من مجموعة واسعة من التهديدات. والتي تتضمن أي شيء ابتداءً من الأخطاء البشرية وتعطل المعدات إلى أن يصل إلى السرقة والاحتيال والأعمال التخريبية من خارج المؤسسة والتخريب المتعمد من قبل العاملين في المؤسسة والحريق والفيضانات وحتى الإرهاب.

وعلى غرار جميع المعايير الأخرى لمنظمة الأيزو. فإن هذا المعيار المنشور لا يقوم حقيقة بوصـف ما هو المطلوب على وجـه التحديد، لكنه يحدد المجـالات التي تحتاج إلى معايير تتعلق بالأمن. الشـكل التوضيحي (٧-٣) يوضح الموضوعات الرئيسـية لمعيار أيزو ٢٧٠٠٢. فالمعيـار لا يحتوي عـلى المتطلبات التفصيلية لـكل من هذه المجـالات - فالمعيار الدولي الشـامل والثابت يتطلب نصاً شاملاً ومكثفاً ولكن لن يكون شاملاً للجميع، وقد يصبح غير صالح. فبدلاً من ذلك على سـبيل المثال. يدعو السـطر (٤-٢) إلى المعايير الأمنية الخاصة بسياسـات وصول الشريك الخارجي أو ما يسـمى الطرف الثالـث Third Party للبيانات. فالأيزو يدعو إلى أن يكون لدى المؤسسـة عمليات موثقة ومعتمدة تشمل السياسات التي تحكـم وصول الشريـك الخارجي أو الطـرف الثالث إلى البيانات والنظـم. لذا يجب على المنشـأة أن تضـع معايير وإجراءات أكثر تفصيلاً خاصة بها في هـذا المجال. إن نوع ومدى هذه المعايير يمكن أن يعتمد على عوامل كثيرة. لذا يجب أن تقوم المؤسسة الممتثلة لمعيار الأيزو ٢٧٠٠٢ بمعالجة هذه القضية جنباً إلى جنب مع المجالات الأخرى في المعيار.

الشكل التوضيحي (٧-٣)

مجالات موضوع معايير الأيزو ٢٧٠٠٢

يسرد هذا الملخص مجالات الموضوعات الرفيعة المستوى الموجودة في هذا المعيار الصادر من منظمة الأيزو (ISO 27002). الخطوط العريضة الفعلية للمعيار تنخفض إلى مستويات متعددة، وأكثر تفصيلاً لكل نقطة من النقاط. هذا المستوى من المخطط التفصيلي يعتبر نموذجاً لجميع معايير الأيزو.

١- النطاق: وصف رفيع المستوى لتطبيق هذا المعيار.

٢- المصطلحات والتعريفات: بما يتفق مع معايير الأيزو الأخرى فإن المصطلحات الرئيسية كافة يتم تعريفها (على سبيل المثال، تعريف المقصود بـ "السرية").

٣- المعايير أو الحاجة إلى سياسة عالية المستوى لأمن المعلومات.

٤- المتطلبات اللازمة للإدارة الأمنية في المؤسسة:

٤-١ البنية التحتية لأمن المعلومات.

٤-٢ السياسات الأمنية ووصول الطرف الثالث.

٤-٣ اعتبارات الاستعانة بمصادر خارجية (اعتبارات التعاقد الخارجي).

٥- معايير تصنيف الأصول والرقابة:

٥-١ المساءلة عن الأصول.

٥-٢ تصنيفات المعلومات.

٦- أمن الأفراد:

٦-١ الاعتبارات الأمنية في تعريفات الوظيفة والموارد.

٦-٢ تدريب المستخدم على أمن الأفراد.

٦-٣ معايير الاستجابة للحوادث الأمنية والأعطال.

٧- الأمن المادي والبيئي، متضمناً ذلك متطلبات لـ:

١-٧ المناطق الآمنة.

٢-٧ أمن المعدات.

٣-٧ الضوابط العامة.

٨- إدارة الاتصالات وعمليات التشغيل:

١-٨ الإجراءات التشغيلية والمسؤولية.

٢-٨ التخطيط والموافقة على النظام.

٣-٨ الحماية ضد البرمجيات الخبيثة.

٤-٨ إدارة الممتلكات.

٥-٨ متطلبات إدارة الشبكة.

٦-٨ معالجة الوسائط والأمن.

٧-٨ تبادل المعلومات والبرمجيات.

٩- التحكم في الوصول:

١-٩ متطلبات الأعمال للتحكم في الوصول.

٢-٩ إدارة الوصول للمستخدم.

٣-٩ مسؤوليات المستخدم بالنسبة للمعايير الأمنية.

٤-٩ التحكم في الوصول إلى الشبكة.

٥-٩ التحكم في الوصول لنظام التشغيل.

٦-٩ إدارة الوصول للتطبيقات.

٧-٩ معايير المراقبة للوصول إلى النظام واستخدامه.

٩-٨ الحوسبة المتنقلة والشبكات ذات الصلة.

١٠- معايير تطوير النظام وصيانته:

١٠-١ المتطلبات الأمنية للأجهزة ونظم البرمجيات.

١٠-٢ أمن نظم التطبيقات.

١٠-٣ ضوابط التشفير.

١٠-٤ أمن ملفات النظام.

١٠-٥ الأمن في عمليات التطوير والدعم.

١١- معايير إدارة استمرارية العمل.

١٢- المعايير الأمنية التي تغطي قضايا الامتثال:

١٢-١ الالتزام بالمتطلبات القانونية.

١٢-٢ مراجعات السياسة الأمنية والتوافق الفني.

١٢-٣ اعتبارات تدقيق النظم.

في خطوة أولى لتطبيق معيار أيزو ٢٧٠٠٢، فإنه يجب على المؤسسة أن تقوم بتحديد احتياجات ومتطلبات أمن المعلومات الخاصة بها. وهذا يتطلب القيام بإجراء تقييم لمخاطر أمن المعلومات على غرار عمليات إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية (COSO)، والتي تم الحديث عنها في الفصل الرابع من هذا الكتاب. يجب أن يركز مثل هذا التقييم على تحديد التهديدات والثغرات الأمنية إلى جانب تحديد الكيفية التي من خلالها يمكن اعتبار كل واحد منها سبباً محتملاً في وقوع الحوادث الأمنية. وينبغي أن تساعد هذه العملية على تحديد الاحتياجات والمتطلبات الفريدة لأمن المعلومات في المؤسسة.

لوضع عمليات خاصة بفرض معيار الأيزو ٢٧٠٠٢ الخاص بأمن المعلومات ينبغي على المؤسسة أن تقوم بتحديد وفهم جميع المتطلبات القانونية والتشريعية والتنظيمية

والتعاقدية التي يجب أن تفي بها المؤسسة ويفي بها أيضاً الشركاء التجاريون والمقاولون ومقدمو الخدمات الذين تتعامل معهم المؤسسة. ويحتاج ذلك إلى فهم وتحديد الاحتياجات والمتطلبات الأمنية الخاصة بالمؤسسة.

يعد أيزو ٢٧٠٠٢ المعيار الأول من بين سلسلة من المعايير الدولية المستهدفة من قبل المؤسسات التي تستخدم نظم الحاسب الآلي الداخلية أو الخارجية، أو التي تمتلك بيانات سرية أو تعتمد على تقنية المعلومات لتنفيذ أنشطة الأعمال الخاصة بها، أو التي ترغب ببساطة في اعتماد مستوى أعلى من الأمان عن طريق التوافق مع المعيار. وتماماً كما أصبح الامتثال لمعايير الأيزو ٩٠٠٠ بمثابة ضمان الجودة، فإن التوافق مع معيار أيزو ٢٧٠٠٢ يُمَكِن الشركاء من أن يكونوا على ثقة في مجمل العمليات الأمنية في المؤسسة. لا بد أن يسهم الامتثال بمعيار أيزو ٢٧٠٠٢ في تعزيز مستوى الثقة المتبادلة بين الشركاء، حيث يمكن لكل منهم إثبات أنه يتبع المعايير الأمنية المتوافقة مع مجموعة من المعايير المعترف بها والمعتمدة عالمياً. عندما يزداد نطاق الامتثال لمعيار أيزو ٢٧٠٠٢ ويصبح أكثر شيوعاً وانتشاراً، فمن الممكن أن يسهم ذلك في انخفاض أقساط التأمين ضد مخاطر الحاسب الآلي، إلا أنه من المؤكد سيوفر مستوى حماية أفضل للبيانات السرية ويحسن من ممارسات الخصوصية والامتثال لقوانين الخصوصية. يعد معيار أيزو ٢٧٠٠٢ منهجية منظمة ومعترفاً بها دولياً تساعد المؤسسة على تطوير إدارة أفضل لأمن المعلومات بصفة مستمرة.

ودعماً لهذا المستوى الرفيع للمعيار الخاص بالضوابط الأمنية، فإن معيار أيزو ٢٧٠٠١ (ISO 27001) وهو ما تعرفه منظمة الأيزو على أنه "مواصفة" خاصة بنظام إدارة أمن تقنية المعلومات. بمعنى أنه قد تم تصميم هذا المعيار لقياس ومراقبة وضبط إدارة الأمن من منظور من أعلى إلى أسفل، إلا أن المعيار أيزو 27001 يوضح كيفية تطبيق معيار أيزو 27002 ويوضح بأن عملية تطبيق هذا المعيار الخاص بأمن المعلومات تتكون من ستة أجزاء:

١- **تحديد السياسة الأمنية:** ثمة عنصر أساسي في أي معيار هو الحاجة إلى بيان بالسياسة الرسمية معتمد من قبل الإدارة العليا. وسيتم قياس جميع جوانب التوافق الأخرى للمعيار مقابل هذا البيان الخاص بالسياسة.

٢- تحديد نطاق نظام إدارة أمن تقنية المعلومات IT security management system (ITSMS):

يعرف معيار أيزو ٢٧٠٠٢ الأمن بعبارات فضفاضة قد لا تناسب أو لا تحتاج إليها جميع المؤسسات. فبعد أن قمنا بتعريف السياسة الأمنية رفيعة المستوى فإن المؤسسة تحتاج إلى تحديد نطاق نظام إدارة أمن تقنية المعلومات IT security management system (ITSMS) النشط الخاص بها. على سبيل المثال، يحدد معيار أيزو ٢٧٠٠٢ عنصراً من عناصر المتطلبات الأمنية كتسجيلات الفيديو والصوت. وقد لا يكون هذا ضرورياً لمؤسسة معينة، ومن ثم سيتم تحديد استبعادها فيما يتعلق بنطاق نظام إدارة أمن تقنية المعلومات (ITSMS) الخاص بها.

٣- **إجراء تقييم المخاطر:** ينبغي على المؤسسة أن تحدد منهجية لتقييم المخاطر تناسب بيئة ITSMS الخاصة بها، وبعد ذلك تقوم بوضع معايير لقبول المخاطر وتحديد ما يمكن أن يشكل مستويات مقبولة من المخاطر.

٤- **إدارة المخاطر:** تعد هذه إحدى العمليات الرئيسية التي تشمل التحديد الرسمي للمخاطر وتحليل المخاطر وخيارات لمعالجة تلك المخاطر. وهذا العنصر الأخير يمكن أن يشمل تطبيق الضوابط المناسبة لتجنب المخاطر وقبول المخاطر واتخاذ خطوات أخرى لتجنبها، أو نقل المخاطر إلى أطراف أخرى مثل شركات التأمين أو الموردين.

٥- **اختيار أهداف الرقابة والضوابط التي سيتم تنفيذها:** تعد هذه الخطوة مشابهة جداً لإجراءات الرقابة الداخلية للإطار (COSO) والتي تمت مناقشتها في الفصل الرابع من هذا الكتاب وكذلك عمليات الرقابة الداخلية في (كوبت) التي نوقشت في الفصل الخامس من هذا الكتاب أيضاً. فلكل هدف من الأهداف الرقابية المعرفة، يجب على المؤسسة أن تحدد الإجراءات الرقابية المناسبة له.

٦- **إعداد بيان الانطباق:** تعد هذه الوثائق الرسمية ضرورية لإنهاء عملية توثيق ITSMS. فمثل هذه الوثائق هي التي تطابق أهداف الرقابة مع الإجراءات الخاصة بإدارة وتنفيذ ITSMS.

وكما هو واضح من هذه الخطوات الست، فإن عملية تحليل المخاطر وتحديد السياسات الأمنية المتبعة يعد من الأمور الرئيسية الهامة بالنسبة لهذا المعيار الخاص بتقنية المعلومات. ونظراً للقواعد الصارمة في حقوق النشر والتأليف الخاصة بالأيزو، فإننا لم نتمكن من إدراج مقاطع محددة من معيار أيزو ٢٧٠٠١ في هذا الفصل. يتم عرض المعايير الفعلية للأيزو في نص محكم واضح لا لبس فيه. ويتم إضافة القليل من التفاصيل المحددة، إلا أن هناك ما يكفي للسماح للمؤسسة بتطبيق النظام الخاص بها لإدارة أمن تقنية المعلومات ITSMS. ويتم اختتام كل معيار بملحق يسرد إجراءات الرقابة الخاصة بتفاصيل كل هدف من أهداف هذا المعيار. ومع ذلك، لا ينبغي النظر إلى معيار أيزو ٢٧٠٠١ على أنه مجموعة شاملة من الإجراءات الرقابية التي سيتم تغييرها بمجرد تغيير التقنية، وإنما هي عبارة عن خطوط عريضة للإطار الخاص بنظام إدارة أمن تقنية المعلومات ITSMS والتي ينبغي تنفيذها ومراقبتها، وصيانتها باستمرار.

يعتبر كل من أيزو ٢٧٠٠١ وأيزو ٢٧٠٠٢ معايير عالمية تحتوي على مخططات جاهزة ومتعارف عليها للامتثال بها والحصول على شهاداتها، خاصة في المملكة المتحدة والاتحاد الأوروبي. وسيستمر كل منها في التطور ومواكبة التقنية والتوسع تبعاً للتغيرات الأكثر شمولية. وتقوم هذه المعايير أيضاً بتوفير الأساس اللازم لتحديد المعايير والممارسات الفعالة في أمن تقنية المعلومات.

معيار أيزو ٣٨٥٠٠ الخاص بحوكمة تقنية المعلومات:

يتم تطوير معايير الأيزو ومن ثم إصدارها في المجالات التي تحتاج بشكل واضح إلى إرشادات تتعلق بأفضل الممارسات الموجودة على المستوى العالمي. في بعض الأحيان يتم إصدار هذه المعايير عندما يكون هناك حاجة تجارية ماسة لتوحيد المواصفات القياسية لمنتج ما. فمعيار أيزو الذي قمنا بالإشارة إليه مسبقاً والذي يتناول موضوع حجم بطاقات الدفع الائتمانية الخاصة بالعميل يعد مثالاً على ذلك. فقد قام مقدمو البطاقات الائتمانية في الأيام الأولى لها بإصدار بطاقات ذات أحجام وأنظمة ترقيم ومواصفات أخرى مختلفة. وبالمثل فقد كانت هناك حاجة إلى معايير خاصة بالعمليات التبادلية لتعزيز التجارة الإلكترونية، وبناء على ذلك تم إطلاق أحد معايير الأيزو الخاصة بهذا الشأن. في بعض

الحــالات الأخرى تمثــل معايير الأيزو أفضل الممارســات عندما يكون الامتثــال بها ضرورياً لأغراض تجارية. ولعل حديثنا الســابق عن معايير الأيــزو ٩٠٠٠ الخاصة بالجودة هو خير مثال على ذلك. تقريباً كل مؤسســات تصنيع المنتجات اليوم التي ترغب في المنافســة على الصعيد الدولي يجب أن يكون مشــهوداً لها بالتوافق مع معايير الأيزو ٩٠٠٠ الخاصة بنظام إدارة الجودة.

عــلى الرغم من أن بعض معايير الأيزو ظلت معمولاً بها لســنوات عديدة. فإن معيار أيزو ٣٨٥٠٠ الخاص بحوكمة تقنية المعلومات يعتبر جديداً نســبياً، وقد تم إطلاقه في عام ٢٠٠٨ بعــد فترة طويلة من التطوير. كما أنه لم يلق في الوقت الحاضر مســتوى جيداً من الاهتــمام الدولي، على الرغم من أن الإصدارات الجديدة المخطط لها للإطار كوبت، والذي تم الحديث عنه في الفصل الخامس من هذا الكتاب سوف تضم المبادئ الخاصة بمعيار أيزو ٣٨٥٠٠. فبالإضافــة إلى إطار الرقابة الداخلية (COSO)، الذي تم الحديث عنه في الفصل الرابــع من هذا الكتاب، والإطــار كوبت، والذي تناولنا الحديث عنــه في الفصل الخامس من هذا الكتاب، وأفضل الممارســات للإطار آيتل الذي تحدثنا عنه في الفصل السادس من هذا الكتاب؛ فإن معيار أيزو٣٨٥٠٠ يعد إطاراً آخر للمســاعدة في دعم الممارسات الفعالة لحوكمة تقنية المعلومات الخاصة بمؤسســة ما. حتى الآن تم إطلاق المعيار على مســتوى عالٍ جداً، أما الأجزاء والإرشادات التفصيلية فمن المؤكد أنها ستأتي لاحقاً. يقدم هذا القسم وصفاً لمعيار أيزو ٣٨٥٠٠ وكيف يمكن أن يســاعد المؤسســة على وضع ممارســات فعالة لحوكمة تقنية المعلومات.

أهداف معيار أيزو ٣٨٥٠٠:

يوفــر هــذا المعيار إطاراً من المبــادئ الخاصة بكبار المديرين لاســتخدامها عند تقييم وتوجيه ومراقبة اســتخدام تقنية المعلومات في مؤسساتهم. وهذا من شأنه أن يساعدهم على فهم الالتزامات القانونية والتنظيمية والأخلاقية المتعلقة باستخدام مؤسساتهم لتقنية المعلومات والوفــاء بها. ويضم الإطار نموذجاً للتعريفات والمبادئ والحوكمة ليحقق ثلاثة أهداف هي:

١- توفير ضمانات لجميع أصحاب المصلحة في المؤسسة في أن يكون لديهم ثقة في حوكمة الشركات في الأمور التي تتعلق بتقنية المعلومات في مؤسساتهم.

٢- إعلام وتوجيه كبار المديرين للتحكم في استخدام تقنية المعلومات في منظمتهم.

٣- توفير أساس لتقييم أهداف حوكمة الشركات فيما يخص تقنية المعلومات.

كما يهدف معيار أيزو ٣٨٥٠٠ إلى إرشاد أولئك المشاركين في تصميم وتنفيذ نظم الإدارة العليا الخاصة بالسياسات والعمليات الفعالة التي تدعم حوكمة تقنية المعلومات. بمعنى أنه، بينما تشير إرشادات هذا المعيار أكثر إلى مستويات الإدارة العليا، فإنه ينبغي على جميع المهنيين المشاركين في تصميم أو تنفيذ أو إدارة أو مراجعة عمليات تقنية المعلومات إعطاء بعض الاهتمام لمثل هذه المعايير الواسعة النطاق.

يُطبق هذا المعيار على حوكمة عمليات إدارة تقنية المعلومات وقراراتها التي يتم التحكم فيها إما من قِبل المتخصصين في تقنية المعلومات داخل المنظمة، أو من قِبل مقدمي الخدمات الخارجيين، أو من قِبل وحدات العمل الأخرى في المؤسسة. يهدف المعيار إلى تقديم دليل إرشادي للمتخصصين في تقنية المعلومات ليقوموا بتقديم المشورة أو تقديم المعلومات أو مساعدة كبار المسؤولين التنفيذيين، مثل:

- كبار المديرين.
- أعضاء المجموعات التي تقوم بمراقبة الموارد داخل المنظمة.
- أخصائيي العمل الخارجي أو التقني مثل القانوني أو المحاسبي.
- الأخصائيين، أو جمعيات تجار التجزئة، أو الهيئات المهنية.
- بائعي الأجهزة والبرمجيات والاتصالات وغيرها من منتجات تقنية المعلومات.
- مقدمي الخدمات الداخليين والخارجيين (متضمناً ذلك استشاريي تقنية المعلومات).
- مدققي تقنية المعلومات.

إن النطاق والأهداف المشار إليها تكون كبيرة إلى حد ما بالنسبة لمعيار جديد وصغير نسبياً. ومع ذلك، هناك بعض المبادئ العامة الرئيسية التي تم وضعها في النص الحالي

الخــاص بها، ويمكننا أن نتوقع أن نرى تعريفات دعم وإرشــادات أكــثر تفصيلاً لمعيار أيزو ٣٨٥٠٠ في السنوات المقبلة.

إطار عمل معيار أيزو ٣٨٥٠٠ لحوكمة تقنية المعلومات:

يحدد المعيار ســتة مبادئ للحوكمة الرشيدة لتقنية المعلومات والتي يمكن تطبيقها على معظم المؤسســات. هذه المبادئ تعبر عن الســلوك المفضل لتوجيه عملية صنع القرارات المتعلقــة بحوكمة تقنية المعلومات. بمعنى أن البيان الخاص بكل مبدأ يشــير إلى ما يجب أن يتم تنفيذه، لكنه لم يحدد كيف أو متى أو بواسطة من سيتم تنفيذ هذه المبادئ، إذ إن هذه الجوانب تعتمد على طبيعة المنظمة التي ستقوم بتطبيق تلك المبادئ:

المبدأ الأول: المســئولية: يتعين على الأفراد والجماعات داخل المؤسســة معرفة وقبول مســؤولياتهم فيما يخص كلاً من توفير وطلب خدمات وموارد تقنية المعلومات. فأصحاب المسؤوليات عن التدابير والإجراءات يملكون أيضاً سلطة تنفيذ تلك التدابير والإجراءات.

المبدأ الثاني: الإســتراتيجية: إســتراتيجية عمل المؤسســة يجب أن تأخذ بعين الاعتبار القدرات الحالية والمستقبلية لتقنية المعلومات؛ حيث ينبغي على هذه الخطط الإستراتيجية لتقنية المعلومات تلبية الاحتياجات الحالية والمستمرة الخاصة بإستراتيجية عمل المؤسسة.

المبــدأ الثالث: الاقتناء: يجب أن تكون أســباب اقتناء عناصر وموارد تقنية المعلومات حقيقيــة ولها ما يبررها، وأن تكون قائمة على أســاس عملية تحليلية مناســبة ومســتمرة، وجاءت نتيجة قرارات واضحة وشــفافة. ويجب أن يكون هناك توازن مناســب بين المنافع والفرص والتكاليف والمخاطر على المدى القصير والطويل.

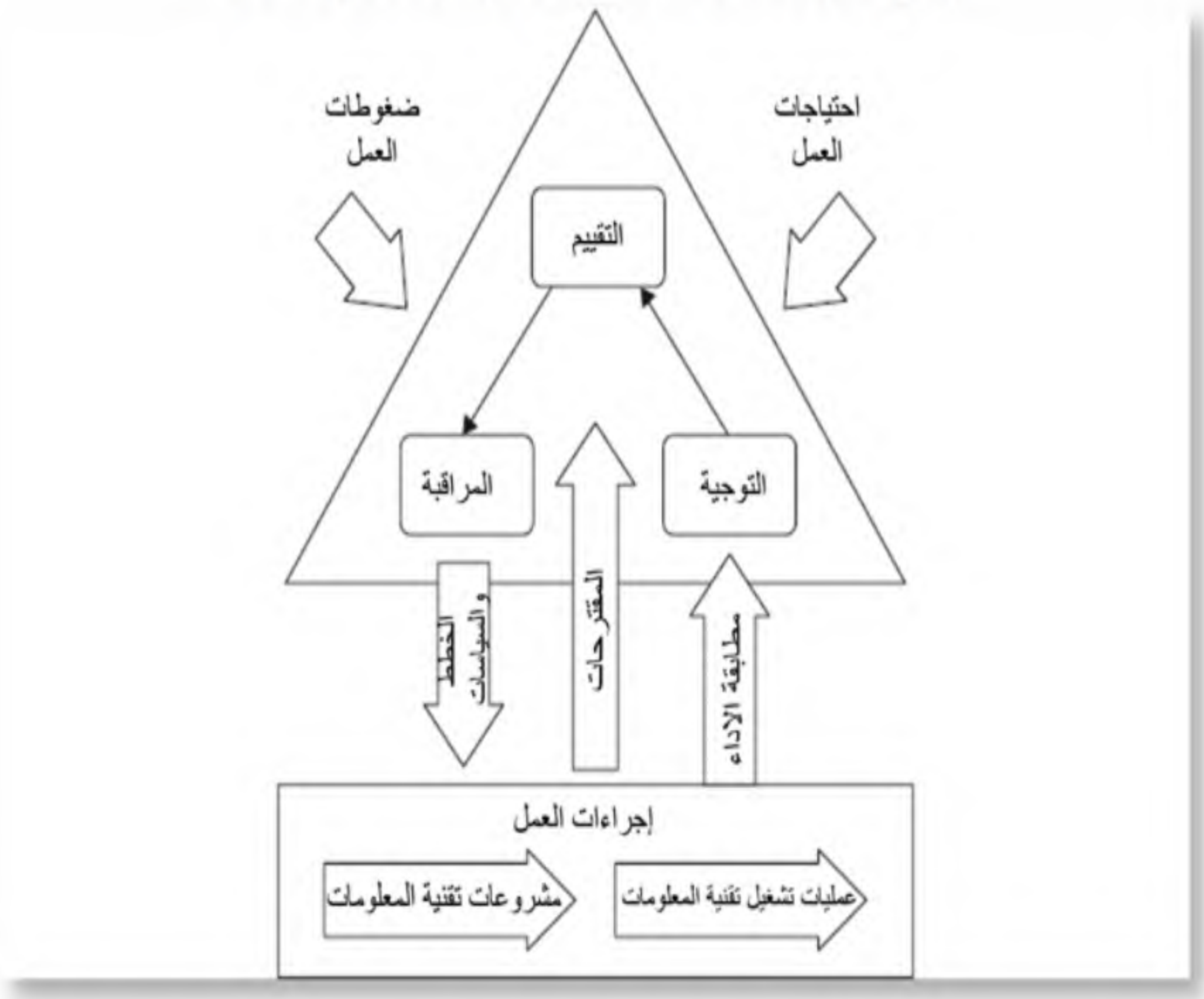
المبــدأ الرابع: الأداء: يجب أن تكون تقنية المعلومات صالحة لأغراض دعم المؤسســة، وتقديم الخدمات، ومستويات الخدمة، وجودة الخدمات اللازمة لتلبية متطلبات المؤسسة الحالية والمستقبلية.

المبــدأ الخامس: الأداء: يجب أن تكون تقنية المعلومــات متوافقة مع جميع القوانين واللوائــح التنظيمية الإلزامية ومع السياســات والإجراءات المحــددة والمطبقة والمفروضة بشكل واضح.

المبدأ الســادس: الســلوك البــشري: يجب على سياســات وإجراءات وقــرارات تقنية المعلومــات أن تُظهِر احترامها للســلوك البــشري، وأن تتضمن جميــع الاحتياجات الحالية والمستحدثة للأشخاص المعنيين في العملية.

شكل توضيحي (٧-٤)

نموذج الأيزو ٣٨٥٠٠ لحوكمة تقنية المعلومات المؤسسية



بالإضافــة إلى تلــك المبادئ الأساســية، فإن المعيــار يقدم أيضــاً نموذجــاً لحوكمة تقنية المعلومات. كما هو موضح في الشــكل التوضيحي (٧-٤). فقد تم وصف العملية الشــاملة لحوكمــة تقنية المعلومــات واحتياجات وضغوطات العمل التي تحتــاج إلى بعض التغييرات والإجراءات في حوكمة تقنية المعلومات في مركز المثلث الموجود في الشكل التوضيحي (٧-٤). يوضح النموذج ضغوطــات واحتياجات الأعمال التي تؤثر في العملية الخاصة بحوكمة تقنية

المعلومات. ثم تأتي بعد ذلك عمليات الحوكمة لتهيمن على مجمل عمليات تقنية المعلومات حيث تتأثر عمليات حوكمة تقنية المعلومات بالمقترحات المختلفة التي نشأت من تقنية المعلومات. كما تقوم عملية حوكمة تقنية المعلومات بتقديم الخطط والسياسات اللازمة لتقنية المعلومات، وتقوم إدارة تقنية المعلومات بأكملها بتقديم معلومات عن أداء وامتثال حوكمة تقنية المعلومات. وقد تم وصف العملية الأساسية الشاملة في فصول أخرى من هذا الكتاب، إلا أن معيار أيزو ٣٨٥٠٠ يقوم بعمل جيد في احتواء هذه المسألة.

يوجد بداخل مثلث حوكمة تقنية المعلومات الموجود في الشكل التوضيحي (٧-٤)، ثلاث وظائف إجرائية هي التقييم والتوجيه والمراقبة. حيث يقدم معيار الأيزو تعريفاً محدداً لكل عملية من هذه العمليات على النحو التالي:

١. **التقييم:** يجب على كبار مديري تقنية المعلومات أن يقوموا بدراسة وإصدار القرارات المتعلقة بالاستخدام الحالي والمستقبلي لجميع موارد تقنية المعلومات. متضمناً ذلك الإستراتيجيات والمقترحات والترتيبات الخاصة بالإمدادات والتجهيزات (سواء كانت داخلية أم خارجية أو كليهما). أثناء تقييم استخدام تقنية المعلومات، ينبغي على الإدارة أن تأخذ في الحسبان الضغوط الخارجية أو الداخلية الناشئة عن الأعمال، مثل توجهات التغير التقني أو التوجهات الاقتصادية أو التوجهات الاجتماعية، والتأثيرات السياسية.

ويجب أن تقوم الإدارة العليا بإجراء هذه التقييمات باستمرار كلما تغيرت ضغوطات الأعمال. ويجب عليها أيضاً أن تأخذ في اعتبارها كلاً من الاحتياجات الحالية والمستقبلية للأعمال - الأهداف التنظيمية الحالية والمستقبلية التي يجب تحقيقها، مثل الحفاظ على الميزة التنافسية. فضلاً عن أهداف محددة للإستراتيجيات والمقترحات التي يتم تقييمها.

٢. **التوجية:** يجب على الإدارة العليا أن تقوم بتخصيص إدارة مسؤولة عن إعداد وتنفيذ الخطط والسياسات، ويجب أن تقوم بنفسها بالإشراف على هذه الإدارة. ويجب على هذه الخطط أن تحدد الاتجاه نحو الاستثمارات في مشاريع تقنية المعلومات وعملياتها التشغيلية. ويجب أن تضع هذه السياسات أسلوباً محدداً وواضحاً في استخدام تقنية المعلومات.

وينبغي أن يضمن المديرون أن عملية الانتقال من المشــاريع إلى الحالة التشــغيلية يتم التخطيط لها وإدارتها بشــكل سليم، مع الأخذ بعين الاعتبار التأثيرات في ممارسات الأعمال والممارسات التشغيلية وكذلك النظم والبنية التحتية الحالية لتقنية المعلومات.

يجب أن تشــجع الإدارة العليــا لتقنية المعلومات على ثقافة الحوكمة الرشــيدة لتقنية المعلومات عن طريق اشــتراط المديرين توفير المعلومات في الوقت المناســب، لتتوافق مع التوجه وتتماشى مع المبادئ الستة للحوكمة الرشيدة.

٣. **المراقبــة:** ينبغــي على الإدارة العليــا أن تراقب، من خلال اســتخدام نظم القياس المناســبة، الأداء العام لتقنية المعلومات. يجب أن يطمئنوا أنفســهم أن هذا الأداء يســير بحســب الخطط المعدة لذلك، وخاصة ما يتعلق بأهــداف العمل. كما ينبغي على الإدارة أيضاً التأكد من أن تقنية المعلومات تتوافق مع الالتزامات التنظيمية والقانونية والتعاقدات الخارجية ومع ممارسات الأعمال الداخلية كذلك.

إرشادات لتطبيق معيار أيزو ٣٨٥٠٠:

قامــت منظمة الأيزو بنشر هــذا المعيار ووضع المبادئ الســت الخاصة به في النموذج الخاص بحوكمة تقنية المعلومات لتقديم إرشــادات أكثر تحديداً لحوكمة تقنية المعلومات. ويمكن شراء هذا الدليل الإرشادي وجميع التفاصيل المتعلقة بالمعيار أو تحميلها من الموقع الإلكــتروني للأيــزو (www.iso.org/iso/catalogue_detail?csnumber=51639). ولا تســمح لنا قوانين حقوق التأليف والنشر الخاصة بالأيزو بإعادة إنتاج هذه الإرشادات التي تــم نشرها. ولكننا قمنا بتحرير واســتخراج جزء صغير من هذه الإرشــادات لتقديم بعض الرؤى عن قرب للمواد الفعلية.

إذا أخذنا مبدأ الإستراتيجية، مثالاً، فإن هناك إرشادات لكل خطوة من الخطوات اللازمة لإجراء التقييم والتوجيه والمراقبة. وعلى الرغم من التغيرات التي طرأت على المعيار الفعلي، وبالتأكيد لم نقصد أن نشرح المعيار الفعلي لأيزو ٣٨٥٠٠، فإن ما يلي يمثل إرشــادات تتعلق بمبدأين من مبادئ المعيار:

- **المبدأ الأول، إستراتيجية لتقييم ما يلي:**

- ينبغي على الإدارة العليا تقييم التطورات الحاصلة في عمليات تقنية المعلومات والأعمال لديهـا لضمان أن تقنية المعلومات سـوف تقدم الدعم الكافي للاحتياجات المسـتقبلية للأعمال.

- إذا أخذنـا بعين الاعتبار الخطط والسياسـات، فعلى الإدارة العليا تقييم أنشـطة تقنية المعلومـات لديها للتأكد من أنها تتماشى مع أهداف المؤسسـة تبعاً للظروف المتغيرة، وتأخذ في الحسـبان ممارسـات أفضل، وتلبـي المتطلبات الرئيسـية الأخرى لأصحاب المصلحة.

- **المبدأ الثاني، إستراتيجية لمراقبة ما يلي:**

- يجب أن تقوم الإدارة العليا بمراقبة التقدم المحرز في المقترحات التي تمت الموافقة عليها لضمان أنها تحقق الأهداف في الأطر الزمنية المطلوبة باستخدام الموارد المخصصة.

- يجب أن تقوم الإدارة العليا بمراقبة استخدام تقنية المعلومات لضمان تحقيقها للفوائد المرجوة.

ويسـتمر المعيار باستخدام هذه اللغة العامة دون وجود أي قواعد محددة أو إجراءات تفصيلية، بل هناك فقط بعض الإرشـادات العامة الجيدة. لكن عندما يدعو المعيار الإدارة العليا "لمراقبة التقدم المحرز في المقترحات التي تمت الموافقة عليها لضمان تحقيقها للأهداف ضمـن الأطـر الزمنية المطلوبة"، فإن هـذا النوع من اللغة يشـير إلى الحاجة إلى إجراءات للموافقة على مشروع وبرنامج تقنية المعلومات وتخطيط للمشروع مع وضع الأطر الزمنية، ومجـرد مراجعات منتظمة من قبل الإدارة العليا. إن إدارة التدقيق الداخلي في المؤسسـة. كما ذكرنا في الفصل التاسـع عشر من هذا الكتاب، يمكن أن تكون بمثابة الخبير الاستشـاري الداخلي الذي يسـاعد في تنفيذ هذه الإرشادات الخاصة بالمعيار، ويتحدث الفصل السادس عشر من هذا الكتاب، على سبيل المثال، عن أهمية إجراءات إدارة المشروعات.

هنـاك العديد من المعايـير الأخرى لمنظمة الأيزو قابلة للتطبيـق في هذا المجال، إلا أن المعيار أيزو ٣٨٥٠٠ يمكن أن يسـاعد ويقوي الحوكمة الشاملة لتقنية المعلومات المؤسسية.

وقــد قام العديــد من المديرين برفض بعض هذه المعايير لأنها كــما يبدو تتطلب وثائق أو أعــمالاً ورقيــة مكثفة أكثر من اللازم. بمعنــى، إذا كان المعيار يقــول: إن «على الإدارة أن تتابع» عملية أو نشــاطاً ما، فإن جماعة المؤسسة التي تدعم هذا المجال يجب أن تكون في وضع يمكنها من إظهار نشــاط المتابعة هذا من خلال مستوى معين من التوثيق. وبالتأكيد فإننا لا نقصد الحديث عن خزائن من العمل الورقي، ولكن نتحدث عن بعض أشكال الأدلة الإلكترونية القابلة للاســترجاع. لقد مرت العديد من مؤسســات اليوم والتي تقوم بتقديم منتجات أو خدمات في الأسواق العالمية من خلال عملية التدقيق الخارجي للأيزو للتصديق عــلى امتثالهــا مع معايير الأيــزو ٩٠٠٠. وقد نرى في الســنوات القادمــة متطلبات امتثال مشابهة لمعايير الأيزو الخاصة بحوكمة تقنية المعلومات عندما تصبح أكثر انتشاراً وقبولاً.

ملاحظات:

١- وليــام إدواردز ديمينج (١٤ أكتوبر ١٩٠٠ - ٢٠ ديســمبر ١٩٩٣) كان أخصائياً، وأســتاذاً ومؤلفاً، ومحاضراً وأستشــارياً أمريكياً، وربما كان الأكثر شــهرة بالنســبة لمجال عمله في اليابان، غير أنه كان زعيم حركة الجودة على مستوى العالم.

٢- Norman Ho, “ISO 9000: No Longer a Stranger to Service,” Gartner, www. qualitydigest .com/june99/html/body_iso_9000.html

الفصل الثامن

قضايا حوكمة تقنية المعلومات: إرشادات حول إدارة المخاطر وإدارة المخاطر المؤسسية الصادرة عن لجنة المنظمات الراعية (COSO ERM) والمجموعة المفتوحة للامتثال والأخلاقيات (OCEG)

تعد إدارة المخاطر أحد المفاهيم المرتبطة بالتأمين، فقد يتصور الفرد أو المؤسسة أن هناك نوعاً ما من التهديد، مثل خطر اندلاع حريق في أحد المباني السكنية أو سرقته، وعندها يقوم باتخاذ الإجراءات اللازمة لتوفير الحماية حال وقوع ذلك التهديد. إن الأسلوب الأكثر شيوعاً للحماية من المخاطر هو شراء تأمين من أحد الموردين الخارجيين التجاريين، أو تركيب آليات حماية للوقاية من المخاطر نوعاً ما. ويتم ذلك باستخدام نهج قائم على المخاطر لتحديد نوع التأمين ومقداره الذي يتم شراؤه أو نوعية الحماية اللازم توفيرها. وتعتمد العوامل الرئيسية لاتخاذ القرار هنا على حجم المخاطر أو التهديدات الأخرى المحتملة، كما تعتمد على تكاليف التأمين والأجهزة الوقائية اللازمة للحماية من تلك المخاطر.

وعلى الرغم من اعتقاد الناس في أغلب الأحيان بأن المخاطر والحماية الوقائية مرتبطة فقط بتهديدات كالحرائق أو الكوارث الطبيعية أو السرقة، فإن المؤسسة تكون في حاجة إلى أن تنظر إلى المخاطر من منظور أوسع من ذلك بكثير، وقد يشمل ذلك أموراً مثل الإخفاق في أحد المشاريع التجارية الجديدة أو الدعاوي الجنائية الناجمة عن عدم نجاح المنتج أو حدوث تحولات اقتصادية سلبية غير متوقعة. ولا تستطيع المؤسسة الحصول على تأمين - فعال وجيد من حيث التكلفة - بتلك السهولة لتغطية تلك المخاطر الأخرى فحسب، بل قد تحتاج إلى تنفيذ عمليات أخرى لتوفير الحماية من تلك المخاطر العديدة والمتنوعة الخاصة بالأعمال. وتكون موارد تقنية المعلومات المؤسسية غالباً أحد أكثر المجالات الرئيسية تعرضاً للمخاطر، حيث تمثل الخسارة المادية لمعدات تقنية المعلومات أو الاضطراب في شبكة الاتصالات أو سرقة مصادر البيانات أحد المخاطر الأساسية التي تهدد المؤسسة وقد يتبعها

عواقــب وخيمة ما لم تكن هناك إدارة مناســبة للمخاطر وأدوات إصلاح قائمة ومعمول بها.

يناقش هذا الفصل أدوات إدارة المخاطر وتقنياتها من حيث أهميتها بالنســبة لحوكمة تقنية المعلومات، كما يقوم أيضاً باســتعراض بعض أساســيات إدارة المخاطر التي يجب أن تمثل إحدى المجالات المعرفية المهمة لدى جميع مديري المؤسســات. ثم يقدم هذا الفصل بعد ذلك إطار إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية (COSO ERM)، وهو إطار متخصص في إدارة المخاطر المؤسسية صادر عن لجنة المنظمات الراعية (COSO) حيث يشــبه إطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية (COSO) — الذي تم عرضه في الفصل الرابع من هذا الكتاب - إلا أن أهدافه مختلفة.

ويُختتــم هذا الفصــل بمقدمة عن نمــوذج الحوكمة وإدارة المخاطــر والامتثال (GRC model) التابع للمجموعة المفتوحة للامتثال والأخلاقيات (OCEG)، مع التركيز على معايير إدارة المخاطــر الخاصة بهذا النمــوذج. وتعمل المجموعة المفتوحــة للامتثال والأخلاقيات (OCEG) وفــق مجموعة من المعايــير الصناعية التي قامت ببناء نمــوذج قدرة الحوكمة وإدارة المخاطــر والامتثال (GRC capability model) الذي يركز بشــكل قوي على إدارة المخاطــر المؤسســية. وقد قامت هــذه المجموعة (OCEG) بإطــلاق مجموعة من المواد الخاصة بأفضل الممارســات في مجال الحوكمة وإدارة المخاطر والامتثال (GRC)، إلا أنها لم تكن بأهمية المعايير نفســها الخاصة بأحكام قانون ساربينز-أوكسلي (SOx instructions) أو معايــير أيــزو. وقد تم مناقشــة كل منهما في فصول ســابقة. ومع ذلــك، فقد تحظى هــذه المجموعة باعتراف وقبول عام في عــالم الصناعة قريباً، وقد يكون الامتثال لمعايير تلك المجموعة أحد الأمور الهامة لحوكمة تقنية المعلومات.

أساسيات إدارة المخاطر:

ســواء تم شراء وثيقة تأمين ضد الحريق لمرفق جديــد بأحد المباني أم تم تثبيت أدوات وقائية لمشروع تجاري جديد أو شراء مســتوى مناســب لما يعرف بالتأمين على مســئوليات المديرين وكبار المسؤولين فى المؤسسة، فعلى الإدارة العليا أن تدرك أنها تتعامل مع مجموعة

متنوعة من المخاطر المؤسسية التي يجب فهمها وإدارتها بشكل مناسب. ويجب التفكير في إدارة المخاطر على أنها عملية من أربع مراحل هي:

١. **تحديد المخاطر:** تحتاج المؤسسة إلى تحديد القضايا والظروف التي يمكن أن تصبح مخاطر مؤثرة في عمليات التشغيل الخاصة بها.

٢. **التقييمات الكمية أو النوعية للمخاطر الموثقة:** الخطوة التي تلي مرحلة تحديد المخاطر المحتملة، وهي توظيف الأدوات لتقدير الآثار المحتملة حال وقوع أي من هذه المخاطر المحددة.

٣. **تحديد أولويات المخاطر وتخطيط الاستجابة لها:** يجب أن تُعطى الأولوية للمخاطر الأكثر تأثيراً من بين المخاطر التي تم تحديدها، كما ينبغي وضع خطط استجابة لهذه المخاطر حال وقوعها.

٤. **متابعة المخاطر:** ينبغي وضع عمليات مستمرة لتقييم الأوضاع الحالية للمخاطر المحددة مسبقاً أو مخاطر جديدة واتخاذ الإجراء المناسب حال وقوع تلك المخاطر وتقييم التقدم المحرز في تلك الإجراءات العلاجية.

وينبغي أن تكون إدارة المخاطر عمليةً تتم على مستوى المؤسسة بأكملها، وتشمل جميع الأشخاص على المستويات كافة وفي جميع وحدات المؤسسة. وبينما تحتاج المؤسسات الكبيرة إلى تشكيل فريق متخصص في إدارة المخاطر، فإنه يجب على المؤسسات الصغيرة تعيين أشخاص ليكونوا مسئولين عن إدارة عملية تقييم المخاطر على مستوى مؤسستهم. فسواء تمت عملية إدارة المخاطر من خلال إدارة رسمية أم بجهود غير رسمية تخدم هذا الغرض، فإنه ينبغي أن تشمل إدارة المخاطر في المؤسسة طائفة عريضة من الناس من مستويات تنظيمية مختلفة في المؤسسة. فقد تكون وجهة نظر المدير المالي التنفيذي حول بعض مخاطر النظم المتعلقة بتقنية المعلومات مختلفة عن وجهة نظر المدير التنفيذي للمعلومات (CIO) أو أحد أعضاء الطاقم الخاص بعمليات تشغيل تقنية المعلومات. فكلٌ منهم يرى المخاطر من وجهات نظر مختلفة. وينطبق هذا التشبيه ذاته على جميع جوانب المؤسسة.

ويجــب تطبيق عمليــة إدارة المخاطر ذات المراحل الأربعة المذكورة ســابقاً على جميع مســتويات المؤسسة وبمشاركة مختلف الأشخاص. فسواء كانت المؤسسة صغيرة بها القليل من المرافق وتقع في منطقة جغرافية محدودة، أم كانت مؤسســة عالمية كبيرة، فإنه ينبغي تطوير أســاليب عامة لإدارة المخاطر، وتعد هذه العملية مهمة وخصوصاً للشركات العالمية المنتــشرة بكثرة هذه الأيام، وهي التي تحتوي على العديد من وحدات التشــغيل المرتبطة بعمليات التشــغيل والمرافق المختلفة الكائنــة في مختلف البلدان. وقد تؤثر بعض مخاطر وحدة تشغيلية معينة في مخاطر وحدة تشغيلية أخرى أو تكون مرتبطة بها بشكل مباشر، غير أن الاعتبارات الخاصة بمخاطر أخرى قد تكون مســتقلةً بشكل فعال عن باقي المخاطر جميعاً. ويمكن أن تقع هذه المخاطر المشــتركة بســبب توافر مجموعة مختلفة وكبيرة من الظــروف تبدأ بقــرارات مالية ضعيفة إلى تغيرات في مدى تجاوب المســتهلكين مع اللوائح الحكوميــة الجديدة. وتعد العمليات الفعالــة لإدارة المخاطر من العناصر المهمة لحوكمة فعالة لتقنية المعلومات.

تحديد المخاطر:

في الوقــت الذي يتم فيه التركيز على حوكمة تقنية المعلومات والمخاطر المتعلقة بتقنية المعلومــات، ينبغي مع ذلك تركيز الإدارة العليا على كل المخاطر التي قد تواجه المؤسســة، ســواء تلك المتعلقة بتقنيــة المعلومات أم غيرها. كما ينبغي أن تســعى الإدارة إلى تحديد جميع المخاطر المحتملة التي قد تؤثر في نجاح المؤسســة، بدءاً من المخاطر الأكبر أو الأكثر تأثيراً بالنسبة لقطاع الأعمال بكاملها، وانتهاءً بالمخاطر الأقل أهمية وهى المرتبطة بالمشاريع الفرديــة أو بوحدات الأعــمال الأصغر حجما. كما تحتاج عملية تحديــد المخاطر إلى اتباع نهــج مدروس للنظــر في المخاطر المحتملة في كل مجال من مجالات العمليات التشــغيلية، ومــن تحديــد مجالات المخاطر الأكثر تأثــيراً والتي يمكن أن تُؤَثِــر في كل عملية خلال فترة زمنية معقولة. ليس المقصود بالفكرة هنا مجرد سرد جميع المخاطر المحتملة، وإنما تحديد المخاطر التي قد تؤثر إلى حد ما في عمليات التشغيل خلال فترة زمنية معقولة. وقد تكون هذه ممارســة صعبة لأننا في كثــيرٍ من الأحيان لا نفهم جيداً احتــمالات وقوع المخاطر أو طبيعة عواقب مواجهة المؤسسة لتلك المخاطر.

يوجد لدى بعض المؤسسات وظيفة مدير تنفيذي للمخاطر يكون مسئولاً عن عمليات إدارة المخاطر في المؤسسة. ويتعين على الإدارة العليا حال غياب هذه الوظيفة أن تبني فريقاً خاصاً بإدارة المخاطر سواء كان ذلك بشكل رسمي أم غير رسمي، وذلك بهدف إدارة عمليات إدارة المخاطر، لديها. كما يجب أن يضم هذا الفريق جميع العناصر الهامة في المؤسسة ومن ضمنهم أعضاء من التدقيق الداخلي والإدارة القانونية والمكاتب الإدارية الرئيسية لقيادة الأنشطة الخاصة بإدارة المخاطر.

كما يجب إتمام عملية تحديد المخاطر التي يقوم بها فريق إدارة المخاطر على مستويات متعددة في المؤسسة. فالمخاطرة التي يكون لها تأثير في وحدة أعمال منفردة أو مشروع مستقل قد لا يكون لها تأثيرٌ كبيرٌ في المؤسسة بأكملها أو خارجها. وعلى العكس من ذلك، فإن إحدى المخاطر الرئيسية التي تؤثر في الاقتصاد بأكمله يمتد تأثيرها ليصل إلى المؤسسة الفردية ووحدات الأعمال المنفصلة التابعة لها. كما قد تكون بعض المخاطر الكبرى نادرة الحدوث، إلا أنها قد لا تزال كارثية بدرجة تجعل من الصعب تحديدها كحدث مستقبلي وارد الحدوث.

إن الطريقة الجيدة لبدء عملية تحديد المخاطر على مستوى المؤسسة هي وضع مخطط هيكلي تنظيمي رفيع المستوى للمؤسسة يسرد المستوى المؤسسي ووحدات التشغيل. وقد يكون لكل وحدة من هذه الوحدات مرافق في مواقع عالمية متعددة، كما قد تتكون أيضاً من عمليات تشغيل عديدة ومتنوعة. ويكون لكل مرفق منفصل بعد ذلك إداراته أو وحداته الخاصة به. وقد تكون بعض هذه المرافق المستقلة مرتبطة بعضها مع بعض بشكل وثيق، في حين يمثل البعض الآخر ما يتجاوز بقليل الاستثمارات التي تعكس التقارير المالية في المؤسسة. وقد يكون من الصعب والمعقد في بعض الأحيان إطلاق مبادرة على مستوى المؤسسة لتحديد جميع المخاطر في مختلف مجالاتها المستقلة. إن هذا النوع من الممارسات يمكن أن يحقق أحياناً نتائج مثيرة للاهتمام و/أو مثيرة للقلق. فعلى سبيل المثال، قد تكون الإدارة على مستوى الشركة على علم ببعض مخاطر المسئولية القانونية عن المنتج، إلا أن مشرف الخطوط الأمامية في وحدة التشغيل قد ينظر إلى المخاطر نفسها من منظور مختلف تماماً.

كما ينظر أعضاء المؤسسة على مختلف المستويات إلى بعض هذه المخاطر ذاتها من وجهات نظر مختلفة. فمدير التسويق قد يشعر بالقلق إزاء إستراتيجيات التسعير الخاصة بالمنافس أو المخاطر الخاصة بأنشطة التسعير التي من شأنها أن تضع المؤسسة في موضع انتهاك للقوانين الخاصة بضبط التبادل التجاري. وقد يشعر مدير تقنية المعلومات بالقلق إزاء مخاطر فيروسات الحاسب أو هجوم البرمجيات الخبيثة على نظم التطبيقات؛ لكنه سيحتفظ بقليل من المعرفة عن تلك المخاطر الخاصة بمسألة التسعير. تكون الإدارة العليا عادة على علم بمستوى مختلف ومجموعة مختلفة من المخاطر أكثر من تلك الموجودة في أذهان فريق العمل المخصص للقيام بعمليات التشغيل. ومع ذلك، يجب على الأقل تحديد كل هذه المخاطر والنظر إليها على أساس وحدة تلو الأخرى وعلى مستوى المؤسسة بالكامل.

وحتى تكون عملية تحديد المخاطر فعالة، يتطلب الأمر أكثر بكثير من مجرد إرسال رسالة بريد إلكتروني إلى جميع مسئولي وحدات التشغيل مع طلب سرد المخاطر الرئيسية في الوحدات التشغيلية الخاصة بهم؛ فمثل هذا الطلب عادة ما ينتج عنه عددٌ كبيرٌ من الإجابات المتعارضة في ظل عدم وجود نهج مشترك. إن أفضل نهج في ذلك هو تحديد أشخاص من مختلف مستويات المؤسسة يُطَالَبُون بأن يكونوا بمثابة مقيمين للمخاطر. لذلك ينبغي تحديد الأشخاص الرئيسيين من داخل كل وحدة من وحدات التشغيل والإدارة المالية وإدارة تقنية المعلومات وإدارة وحدة الأعمال. ويكون هدفهم جميعاً هو تحديد المخاطر في وحداتهم ثم المساعدة في تقديرها، تلك المخاطر التي تقع حول إطار نموذج تحديد المخاطر. ويمكن أن يقود هذا النوع من المبادرات مجموعة خاصة بإدارة المخاطر على مستوى المؤسسة، إن وجدت، أو يُضاف ضمن مهام إدارة تقييم الضوابط الداخلية مثل التدقيق الداخلي.

ولعل أحد الأساليب الفعالة هنا هو تحديد بعض مجالات مخاطر "المغالطة البهلوانية"(*) Straw man العالية المستوى التي قد تؤثر في وحدات التشغيل المختلفة. ويمكن للأشخاص ذوي المعرفة بعد ذلك أن ينظروا في هذه المخاطر القائمة على الإفتراض، كما يمكنهم أيضاً توسيعها بإضافة المزيد من المخاطر إليها أو التعديل عليها إذا اقتضى الأمر ذلك. ويوضح

(*) المغالطة البهلوانية أو رجل القش هي إحدى الادعاءات القائمة على تحريف الموقف المعارض، بتفنيد شكل الحجة بحيث يوحي أن الحجة المعاكسة صحيحة. ويقصد بها هنا تحديد المخاطر المحتملة من وجهة نظر معينة ومن ثم استخدام ذلك كأساس تنطلق منه ورش عمل يتم عقدها بين المعنيين بهذا الأمر للعمل من "رجل القش" هذا نحو ما يعتقدون أنه المخاطر المحتملة (المترجم).

الشــكل التوضيحي (٨-١) مثالاً لعينة من إطار عمل نموذج المخاطر المؤسســية، فهو يسرد بعض مجــالات المخاطر الرئيســية التي قد تؤثر في المؤسســة، مثل المخاطر الإســتراتيجية ومخاطر عمليات التشــغيل والمخاطــر المالية. وتعد تلك العينة أحد أنــواع القوائم عالية المســتوى التي قد يتعجل الرئيس التنفيذي بوضعها رداً على سؤال يطرحه أصحاب المصالح خلال الاجتماع الســنوي مثل، "ما الذي يقلقك نهاية اليــوم؟" لكنه بالتأكيد لا يسرد جميع المخاطر التي تتعرض لها المؤسســة، وإنما يعد هذا نوعاً من أنواع القوائم الأولية التي يمكن للمؤسسة استخدامها للبدء في عملية تحديد المخاطر تفصيلياً. ويمكن أن يجتمع المسئولون في المؤسسة - وغالباً يكون الفريق المعين لإدارة المخاطر - مع الإدارة العليا ويقومون بطرح بعض الأسئلة من نوعية "ما يقلقك؟ ..." لتحديد تلك المخاطر العالية المستوى.

إن هذا النموذج العام الذي يتعلق بالمخاطر العالية المستوى على وجه الخصوص يمكن أن يعمل أساســاً لتحديد مخاطر معينة تواجه مختلف وحدات المؤسسة على نحو أفضل. فعلى ســبيل المثال، يقوم النموذج بإدراج "مخاطر اســتمرارية الأعمال" تحــت "المخاطر التقنية". وينبغــي أن يكــون مدير تقنية المعلومات قادراً على توســيع هذه المخاطر لتكون في شــكل قائمة طويلة من المخاطر التقنية التفصيلية المتعلقة باستمرارية الأعمال والتعافي من كوارثها. ويُعد مدير عمليات التشغيل هو مستخدم موارد تقنية المعلومات الذي قد ينظر إلى مخاطر استمرارية الأعمال من وجهة نظر مختلفة جداً ويعرض مخاطر أخرى جديدة مرتبطة بما قد يحدث إذا لم تُتَح خدمات تقنية المعلومات. ولفهم أفضل للمخاطر التي تواجه المؤسسة، فإنه يكون من الأفضل غالباً توسيع تلك القوائم لوضع مجموعة أكثر اكتمالاً للمخاطر المحتملة.

التقييم الكمي أو النوعي للمخاطر:

نشــير هنا إلى خطوة هامــة للغاية في عملية تقييم المخاطر وهــي أخذ جميع المخاطر المحــددة وترتيبها من حيث تأثيرهــا واحتمالية حدوثها. حيث تُوجــد العديد من الطرق الرســمية التي يمكن اســتخدامها هنا وتكــون غالباً معقدةً رياضياً، ولأننــا لا نقوم بتحليل محطة توليد كهرباء ممولة من الحكومة أو ما شــابه ذلك، فإن المؤسسة تكون غالباً أفضل حالاً إذا ما اســتخدمت نهجاً بســيطاً ومباشراً لتقييم المخاطر بحيــث يفهمه جميع أعضاء فريق الإدارة العليا المسئولة عن عملية إدارة المخاطر الخاصة بهم ويقبلونه.

شكل توضيحي (٨-١)

أنواع مخاطر الأعمال المؤسسية

	المخاطر الإستراتيجية	
مخاطر العوامل الخارجية		مخاطر العوامل الداخلية
• مخاطر الصناعة		• مخاطر السمعة
• مخاطر الاقتصاد		• مخاطر التركيز الإستراتيجي
• مخاطر المنافس		• مخاطر دعم الشركة الأصل
• مخاطر التغييرات القانونية والتنظيمية		• مخاطر حماية براءات الاختراع / العلامات التجارية
• مخاطر احتياجات العملاء ورغباتهم		
	مخاطر عمليات التشغيل	
مخاطر العملية	مخاطر الإمتثال	مخاطر الموظفين
• مخاطر سلسة التوريد	• مخاطر بيئية	• مخاطر الموارد البشرية
• مخاطر رضا العميل	• مخاطر تنظيمية	• مخاطر تنقل العمالة
• مخاطر زمن الدورة	• مخاطر السياسات والإجراءات	• مخاطر حوافز الأداء
• مخاطر تنفيذ العملية	• مخاطر التقاضي	• مخاطر التدريب
	المخاطر المالية	
مخاطر الخزينة	مخاطر ائتمانية	مخاطر تجارية
• مخاطر أسعار الفائدة	• مخاطر السعة	• مخاطر السلع الأساسية
• مخاطر صرف العملات الأجنبية	• مخاطر الضمان	• مخاطر فترة التنفيذ
• مخاطر توفر رأس المال	• مخاطر التركيز	• مخاطر القياس
	• مخاطر التعثر (التخلف عن السداد)	
	• مخاطر التسوية	

مخاطر البنية التحتية ونظم تقنية المعلومات		
مخاطر مالية	مخاطر تشغيلية	مخاطر تقنية
• مخاطر المعايير المحاسبية	• مخاطر التسعير	• مخاطر الوصول إلى المعلومات
• مخاطر إعداد الميزانية	• مخاطر قياس الأداء	• مخاطر استمرارية الأعمال
• مخاطر إعداد التقارير المالية	• مخاطر سلامة الموظف	• مخاطر الإتاحة
• مخاطر الضرائب		• مخاطر البنية التحتية
• مخاطر إعداد التقارير الرقابية		

وكما أوضحنا قبل قليل، فأنه يجب أولاً على المؤسسات ووحدات تشغيل الأعمال التابعة لهــا تحديد جميــع المخاطر المؤثرة التي تواجه المؤسســة بكاملها. وينتــج غالباً عن هذه الممارسة الخاصة بتجميع قائمة كهذه مجموعةٌ كبيرةٌ من المخاطر المحتملة يكون بعضها في كثــير من الأحيان خارج نطاق فهم الإدارة العليا أو تقديرها. فمدير تقنية المعلومات، على ســبيل المثال، قد يسلط الضوء على أحد المخاطر في إستراتيجية البنية الموجهة نحو خدمات تقنيــة المعلومات في المؤسســة، كما أوضحنا في الفصل الثالث عــشر من هذا الكتاب، وهو الأمر الذي قد لا تفهمه أو تقدره الســلطة التنفيذية للمؤسســة. وهنا يمكن لإدارة تقنية المعلومــات أن تتقصى مدى تأثير هذه المخاطرة وســبب المطالبة بمزيد من الموارد للتصدي لهــا. وعلى أية حال، يجب أن تحتفــظ الإدارة العليا بنهج توافقي تنظر من خلاله إلى مثل تلــك المخاطر وكذلك إلى التكاليف المرتبطــة بوضع الإجراءات التصحيحية لها. وبعد ذلك يجب عليهم موازنة هذه المخاطرة مع العديد من المخاطر الأخرى التي قد تم تحديدها.

وعــلى الرغم من أن هناك العديد من الأســاليب الرســمية المنشــورة والخاصة بالعملية الرســمية لتحليل المخاطر، فإن المؤسسة تحتاج إلى نهج بســيط لكنه دقيقٌ لتنظر من خلاله في جميــع المخاطر التي تم تحديدها لتقــرر أيٌّ منها يحتاج إلى إجراءات تصحيحية ومتابعة. ويمكن استخدام مجموعة متنوعة من الأساليب، تمتد من النهج الكيفي السريع نسبياً القائم على التخمين الأفضل وصولاً إلى بعض الأساليب الكمية التفصيلية والرياضية الخالصة. وتتضح الفكرة الكلية هنا في مســاعدة الإدارة على اتخاذ قرار أفضل فيما يتعلق بأي من تسلســلات الأحداث المحتملة المحفوفة بالمخاطر التي قد تمثل القلق الأكبر لإدارة المؤسسة.

إن النهـج البسـيط الذي يكون فعالاً غالباً هو تبني قائمة المخاطر السـابق مناقشـتها وتعميمها على جميع المشـاركين، ويتم في ذلك تحديد المخاطر أو غيرها من خلال اسـتبيان يسأل عن كل مخاطرة من تلك المخاطر:

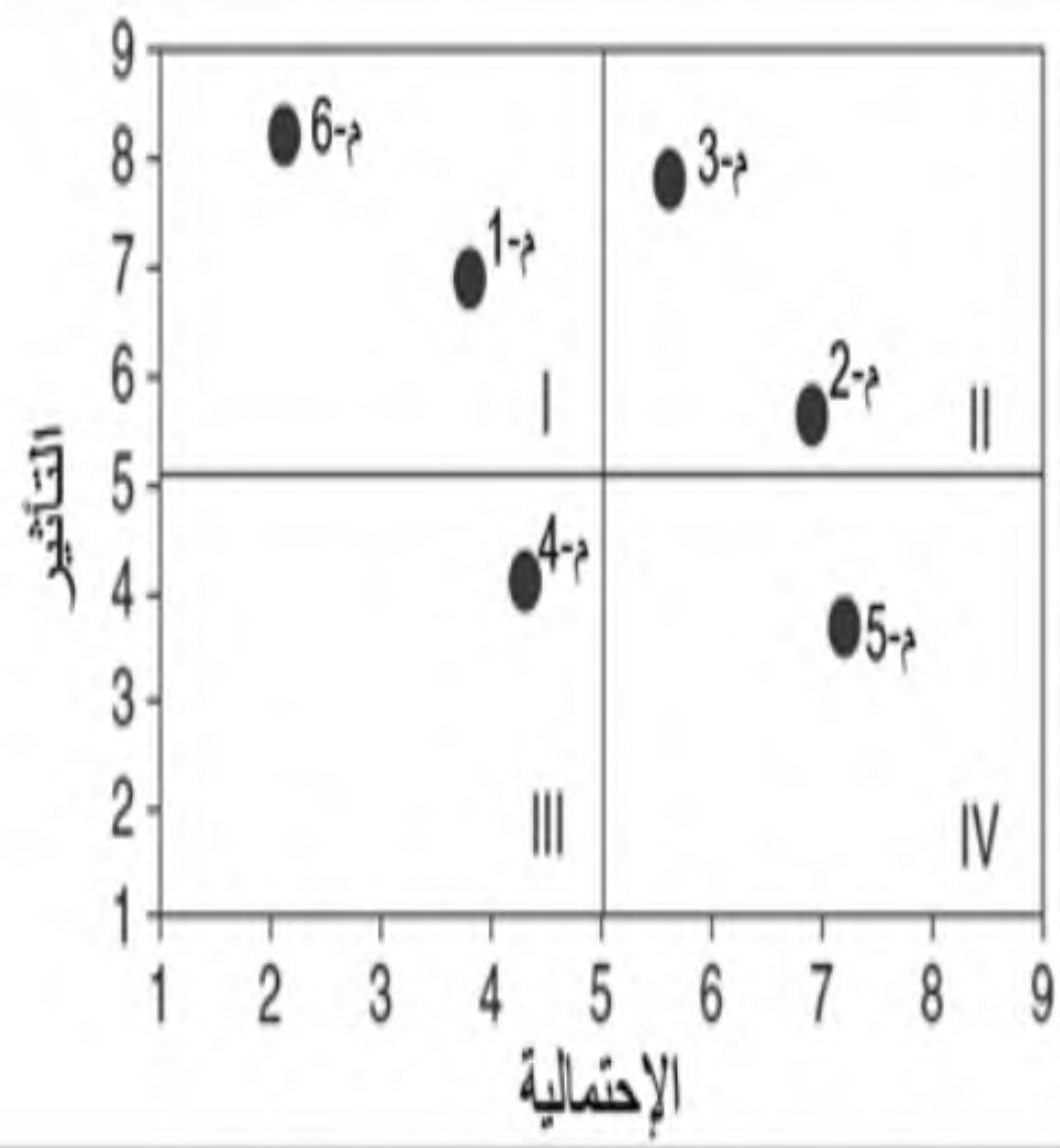
- ما مدى احتمالية حدوث مخاطرةٍ ما خلال السـنة القادمة تحديداً؟ مستخدماً الدرجات من ١-٩، قم بوضع درجة من رقم واحد لأفضل تخمين على النحو التالي:
  - الدرجة ١ إذا كنت لا ترى تقريباً أي فرصة لحدوث هذه المخاطرة خلال تلك الفترة.
  - الدرجة ٩ إذا كنت تشعر أن هذا الحدث سيحدث بشكل شبه مؤكد خلال تلك الفترة.
  - الدرجات من ٢ إلى ٨ تعتمد على شعورك بأن الاحتمالية تقع بين هذين النطاقين.
- ما مدى تأثير المخاطرة من حيث التكلفة على المؤسسـة؟ مرة أخرى باسـتخدام المقياس من ١-إلى-٩، ينبغي أن تعتمد نطاقات الدرجات على التأثير المالي للمخاطرة في المؤسسة. فالمخاطرة التي يمكن لتكاليفها أن تخفض أرباح المؤسسـة حتى سـنت واحد للسهم قد تكون مؤهلة للحصول على أقصى درجة، ٩.

ويجب توزيع الاسـتبيانات الخاصة بهذا النهج المبسـط بشـكل مستقل على الأشخاص ذوي المعرفة لتقييم كل مخاطرة من المخاطر التي تم تحديدها بالنسـبة لهذين المقياسـين (احتمالية الحدوث والتأثير) أو وضع درجة لها. ومثالاً على ذلك، لنفترض أن المؤسسة قامت بتحديد ستة مخاطر من م-١ إلى م-٦، وأنه يُطلب من أعضاء الفريق الخاص بتقييم المخاطر إجـراء تقييم منفصل لكل مخاطرة من تلك المخاطر على حدة من حيث مقاييس احتمالية الحـدوث والتأثـير. بعد ذلك ومن خلال تطبيق هذين العاملين يُحسـب متوسـط هذه الدرجات، كما يتم رسـمها على مخطط الرسـم البياني، ذي الأجزاء الأربعة، الخاص بتحليل تقييم المخاطر كما هو مبين في الشـكل التوضيحي (٨-٢). حيث يُظهِر أن م-١ لها متوسط درجة احتمالية حدوث نحو ٣,٧٥ ودرجة تأثير ٧,٠٠، ويتم رسم هذه الدرجة في الربع الأول مـن المثال الخـاص بمخطط تحليل تقييم المخاطر. ويدل هـذا على أن م-١ تعتبر مخاطرة مؤثرة نسبياً لكن احتمالية حدوثها بعيدة جداً.

ويجب رسم جميع المخاطر التي يتم تحديدها بهذه الطريقة. فالمخاطر ذات احتمالية حـدوث عالية وأكثر تأثـيراً التي تنتهي في الربع الثاني، يجـب أن تلقي المزيد من الاهتمام الفوري من قبل الإدارة.

شكل توضيحي (٨-٢)

مخطط تحليل تقييم المخاطر



وتعـد النطاقـات من ١ إلى ٩ هنـا اعتباطية جداً؛ لذا ينبغي أن تحدد المؤسسـة بعض الخطوط الإرشـادية النسـبية، لكن يجب عـلى الموظفين فقط تقييم الأمـور وفق رؤيتهم لاحتمالية الحدوث والتأثير النسـبي للمخاطر التي تـم تحديدها. كما يقدم هذا المخطط البيـاني الخاص بتحليل تقييم المخاطر مقياسـاً كيفياً جيداً لفهـم المخاطر المؤثرة المحيطة بالمؤسسة.

إن ما قامت به عملية تقييم المخاطر لا يتعدى وصف الأعمال التي تحتاجها المؤسسـة عندما تقوم بتحديد عدد قليل نسبياً من المخاطر بشكل جيد. فمن السهل تماماً أن ننظر إلى الرسـم البيـاني الخاص بتحليل تقييم المخاطر والتركيز عـلى المخاطر العالية الاحتمالية

والتأثـير في الربع الثاني - الأيمن العلوي - للتركيز عـلى وضع خطط الإصلاح لتلك المخاطر. وعلى أية حال، فإنه في كثير من الأحيان، إذا كانت المؤسسة قد حددت مجموعةً أكبر بكثير من المخاطر المحددة ومن النطاقات (من ١-٩) وكذلك المخططات في مثال الرســم البياني، فـإن الرســم البياني لن يوفر تفاصيل كافية. ومن ثــم فالنهج الأفضل هو التعبير عن هذه التقديــرات المهمة والمؤثرة بدلالــة عدد مكون من رقمين يمثل تقدير نســبة مئوية (على سبيل المثال، ٧٢٪) من تحقيق مخاطرة ما أو احتمالية (على سبيل المثال، ٠,٧٢).

كــما أن مجرد زيادة عدد الأرقام في النســبة مثــلاً (٠,٧) او (٠,٧٢) لــن يزيد من دقة التقييم، لكنه يشير إلى أن فريق تقييم المخاطر يجب أن يكرس مزيداً من الاهتمام للحصول على تقديرات دقيقة. كما أن ذلك يساعد فرق التقييم في فهم العلاقة بين الاحتمالات التي تغطي الأحداث المستقلة وذات الصلة على نحو أفضل.

و عــلى أية حال، تحتــاج العملية الدقيقة لتقييم المخاطــر إلى ما هو أكثر من مجرد تقديرات "التقديرات المرتفعة" ســواء كانت ممثلة بنطاق مفرد (١-٩) أم نســبة مئوية كاملــة من رقمين. كما يجب على فريــق تقييم المخاطر وغيرهم من المهتمين أن ينظروا بحــرص في المخاطر التــي تُحدَّد أثناء عمليــة تحديد المخاطر، وينبغــي جمع مزيد من المعلومات، إذا لزم الأمر. فعلى ســبيل المثال، أثناء عملية تحديد المخاطر، قد يعتبر أحد المديريــن أن الآثار المترتبة عــلى القانون الجديد للتعرفة الجمركيــة يعد بمثابة مخاطرة مهمة، وربما يقوم آخرون في الجلســة نفسها بتوسيع التبعات بإضافة المزيد من المخاطر واعتبــار أن القانــون المفترض والمرتقب يعد بمثابة مخاطرة مؤثــرة. وعلى أيةِ حال، قبل وضــع التصنيــف القائم على الأهميــة والتأثير، قد يرغب الفريق أو غــيره من المديرين المسؤولين في القيام بمزيد من الأبحاث لتحديد التبعات الفعلية. ولربما في بعض الأحيان لا تكون هذه التبعات قابلة للتطبيق على الوحدة التشــغيلية التي نحن بصدد الحديث عنهــا، أو أنه لن يكون لهــا أي تأثير يذكر حتى على مدار عدة ســنوات قادمة. وتتضح النقطة الأساسية هنا في أن كل المخاطر التي تُحدد قد تحتاج إلى بعض المعلومات الإضافية لضمان تطبيقها بدقة.

تخطيط الاستجابة للمخاطر:

تَظهر قيمةٌ متواضعةٌ حال نشر قوائم تفصيلية عن المخاطر المؤثرة ما لم تقم المؤسسة على الأقل باتخاذ بعض الخطوات الإجرائية الأولية إن (أو عندما) تتحمل المخاطرة. وتتضح الفكرة هنا في تقدير أثر تكلفة تحمل بعض المخاطر المحددة ومن ثم تطبيق تلك التكلفة على احتمالية عامل المخاطرة الخاص بالمخاطرة لاستنتاج القيمة المتوقعة للمخاطرة. كما يمثل هذا وقتاً مهماً لتحديد من هو المالك أو المسئول عن المخاطرة ومن هو الشخص أو الجهة المسئولة عن معرفة حالة المخاطرة المحددة ومتابعتها. ولا يحتاج هذا الإجراء في كثير من الأحيان إلى دراسات تفصيلية للتكاليف ولا إلى كثير من الاتجاهات والتقديرات التاريخية الداعمة. فقد تم تحديد المخاطر الخاصة بنا من خلال نهج العصف الذهني السريع الاستجابة دون تحليل تفصيلي، وبعد ذلك يقوم أشخاصٌ ذوو معرفة بإجراء تقديرات احتمالية الحدوث والتأثير في ظل وجود المعرفة العامة عن المجال. كما يجب الانتهاء من حساب التكاليف المتوقعة، ويقوم بذلك العاملون في الخطوط الأمامية ويشملون أشخاصاً على مختلف مستويات المؤسسة يكون من المتوقع احتفاظهم ببعض المعرفة.

وتتضح الفكرة هنا من خلال المرور على كل مخاطرة تم تحديدها — وإذا كان الوقت محدوداً، فإنه يكفي فقط المرور على المخاطر الرئيسية — وتقدير تكاليف تحمل المخاطر المحددة. ويوضح الشكل التوضيحي (٨-٢) ست عينات لمخاطر تم رسمها باستخدام التقديرات الخاصة باحتمالية الحدوث والتأثير لكل مخاطرة. وهنا تمثل النواتج المشتركة لحاصل ضرب التأثير والاحتمالية درجة من درجات تقييم المخاطرة، وبترتيب هذه الدرجات تصبح القيمة الأعلى هي عنصر المخاطرة الأكبر الذي يدعو للقلق والاهتمام.

ويجب على فريق تقييم المخاطر النظر في أثر تكلفة كل مخاطرة من المخاطر المحددة وتقدير التكلفة الإجمالية على المؤسسة حال وقوعها. كما يوجد العديد من الطرق لوضع مثل هذه التقديرات الخاصة بتكلفة المخاطر، إلا أنه يجب استخدام النهج نفسه مع جميع المخاطر التي تم تحديدها. وبناءً على ذلك، يصبح حاصل ضرب درجة المخاطرة وتأثير التكلفة هو التكلفة أو الخسارة المتوقعة التي ستتكبدها المؤسسة حال وقوع المخاطرة

المحـــددة. ويوضح الرســـم البياني في المثـــال أنه على الرغم من أن المخاطـــرة م-٥ بها أعلى احتمالية حدوث، فإن تأثير التكلفة الأعلى للمخاطرة م-٢ قد يســـبب قلقاً إدارياً أكبر بكثير من المخاطرة م-٥.

مـــن المؤكد عدم دقة عينـــة تحليل المخاطر هذه، إلا أنها توضح أحد أنواع التفكير الذي نحتـــاج إليه لتقدير تكاليـــف التعافي من بعض وقائع المخاطـــر. في كثير من الأحيان يكون من الســـهل التعرف على بعـــض وقائع المخاطر، لكن الأكثر صعوبـــة في الغالب هو تحديد تكلفـــة التعافي من تلك المخاطرة. وعلى النحو المقـــترح طوال هذا الفصل، لا توجد حاجة لإجراء تحليلات تفصيلية تستغرق الكثير من الوقت، بل يكفي الاستعانة بأهل العلم الذين يفهمـــون مجال المخاطرة لإعطـــاء بعض التقديرات. كما يتعين على الفرق في الكيانات التي قد تتحمل هذه المخاطر المحددة أن تقدر التكاليف على أُسس هي:

- تقدير التكلفة لأفضل الحالات التي يكون من الضروري فيها تحمل المخاطرة. يظهر هذا الافتراض فقط في حال وجود تأثير محدود عند حدوث المخاطرة.
- تقدير تكلفة العينة التي يقوم بها الشخص صاحب المعرفة.
- القيمـــة أو التكلفـــة المتوقعة لتحمل المخاطرة. هذا هو نوع المخاطرة الذي قد يشـــمل تكاليف أساسية وغير ذلك من العوامل مثل العمل الإضافي.
- تقدير التكلفة لأســـوأ الحالات التي يكون من الضروري فيها تحمل المخاطرة. ويعد هذا أحد أنواع التقدير "إذا كان كل شيء يسير على نحو خاطئ".

لقد اقترحنا اســـتخدام هذه التقديرات نقطة بداية لتشـــكيل فكرة عن حدود التكاليف التي تدور في خلد مختلف الأفراد، ومع ذلك فإننا نؤكد أن هذا مجرد نهج عالي المســـتوى. ويجـــب أن تعمـــل الإدارة العليا مع فرق الدعم المســـئولة عن تقييـــم المخاطر لديها لفهم العمليات المعمول بها في المؤسسة.

ويعـــد الشـــكل التوضيحي (٨-٣) مثالاً عـــلى تخطيط ترتيب المخاطـــر. فخلية "القيمة المتوقعة" ليســـت ســـوى حاصل ضرب خلايا "أثر التكلفة" و"درجة المخاطرة". ويُقَدِر هذا الرقم التكلفة التي ســـتتكبدها المؤسســـة حـــال تحملها مخاطرة ما. وعـــلى الرغم من أن

الأرقام التي اختيرت لهذه العينات أرقام اعتباطية، فإنها توضح للمديرين أو أخصائيي إدارة المخاطر المؤسسية (ERM) كيفية تفسير هذه النوعية من التحاليل والعمل بمقتضاها.

فالمخاطرة م-٣، على سبيل المثال، بها احتمالية عالية وتأثير عالٍ، وكذلك التكلفة المتوقعة للتصحيح تكون عالية نسبياً. كما أن هذا النوع من المخاطر هو الذي ينبغي أن تحدده الإدارة على أنها أحد المخاطر المرشحة لاتخاذ إجراءات تصحيحية حيالها. ومع ذلك، فإن المخاطرة التالية في الجدول، المخاطرة م-٢، تنتمي أيضاً إلى الجانب الأيمن العلوي من الشكل الرباعي لكن بتكلفة عالية نسبياً لمعالجتها. وقد يكون هذا أحد نوعيات المخاطر التي بناءً عليها ستقرر الإدارة إذا ما كانت ستقبل المخاطرة أو تطور شكلاً آخر من خطة العلاج كما سيتم مناقشته لاحقاً.

شكل توضيحي (٨-٣)

مثال تخطيط الاستجابة طبقاً لتقييم المخاطر

المخاطرة	التأثير	الاحتمالية	درجة المخاطرة	التقييم	أثر التكلفة	قيمة الخسارة المتوقعة للمخاطرة
م-٣	٨,٠	٥,٧	٤٥,٦	١	١٢٠,٦٠٠$	٥,٤٩٩,٣٦٠ $
م-٢	٥,٥	٧,٠	٣٨,٥	٢	٧٨٥,٠٠٠$	٣٠,٢٢٢,٥٠٠$
م-٥	٣,٩	٧,٢	٢٨,١	٣	١٥,٠٠٠ $	٤٢١,٢٠٠ $
م-١	٦,٨	٣,٨	٢٥,٨	٤	٢٧,٢٥٠ $	٧٠٤,١٤٠ $
م-٤	٤,٢	٤,٣	١٨,١	٥	٥٢,٣٥٠ $	٩٤٥,٤٤١ $
م-٦	٨,٤	٢,٠	١٦,٨	٦	١,٢٠٠ $	٢٠,١٦٠ $

ونؤكد مرة أخرى ارتفاع تكلفة المخاطرة، وفي هذه الحالة يكون تأثيرها مرتفعاً نوعاً ما، لكن احتمالية حدوثها تكون منخفضة للغاية. وهذه هي نوعية الأرقام التي تقرر الإدارة غالباً من خلالها أن "تأمل خيراً" وتعيش مع المخاطرة. وبالنسبة لمثل تلك المخاطرة، فإنها ستكلف الإدارة إذا ما قررت تحملها، كما ستكون مُكلِّفةً حال تثبيت بعض الأدوات الخاصة بالإجراءات التصحيحية. وعلى افتراض أن فريق إدارة المخاطر المؤسسية قام بعمل جيد في

إعــداد تقديــرات المخاطر تلك التي تم تحديدها، فهذا يمكن أن يكون نهجاً مفيداً في اتخاذ القرارات المتعلقة بالمعالجة المستمرة للمخاطرة.

متابعة المخاطر:

بينما يلزم عمل مسح للمخاطر المحتملة في البيئة المؤسسية ثم تقدير تكاليف واحتمالات تلــك المخاطر التي قد تحــدث، فإنه يلزم القيام بهذا الإجراء لأكثر من مرة. بل يجب وضع عمليات رسمية لمتابعة المخاطر وفحص حالتها، فضلاً عن معرفة المخاطر الجديدة المحتملة بشــكلٍ مســتمر. إن متابعة المخاطر هي عملية توصيف الوضع الحالي للمخاطر المحددة وتحليله وكذلك تتبع المخاطر الجديدة المحتملة حال ظهورها. فهي تضمن أن موارد الشركة المخصصة للمشروع تعمل بشكل صحيح.

إن هــذا المفهوم الخاص بتثبيت أدوات متابعة ســيظهر في كثير من العمليات الأخرى الخاصة بحوكمة تقنية المعلومات التي تمت مناقشتها في فصول لاحقة. فعلى سبيل المثال، يناقش الفصل الرابع عشر مــن هذا الكتاب إدارة حوكمة تقنية المعلومات وإدارة محفظة استثمارات تقنية المعلومات، في حين يقدم الفصل السادس عشر من هذا الكتاب للقارئ، ما يعرف بالإدارة الفعالة لمحفظة المشاريع والبرامج. وفي تلك الحالات وغيرها، تحتاج المؤسسة إلى وضع ضوابط رقابية لتقييم الحالة بشكل مستمر.

وفي الماضي لم تكن العديد من أدوات المتابعة هذه موجودةً بشكل واقعي في العديد من مجالات النظم التقليدية مثل تقنية المعلومات. فقد كان طاقم تقنية المعلومات في كثير من الأحيان يترقبون بكل أمل أن تسير الأمور بسلام وألا تتعطل النظم الرئيسية. وإذا ما حدث ذلــك وتعطلت تلك النظم وما يصاحبها من تداعيــات، تظهر عادةً حالةٌ من الزخم تهدف إلى استعادة تلك النظم للعمل مرة أخرى. وفي السنوات الأخيرة فقط تم وضع العديد من أفضل تطبيقات تقنية المعلومات التي تم اســتخدامها وتطبيقها مع أدوات متابعة لتسليط الضوء على حالات المشاكل.

كان لدينا تجربة أفضل بكثير مع أدوات المتابعة في بيئة إدارة المخاطر، إذ كلٌّ من إنذار الحريق التقليدي المثبت على الحائط أو جهاز الإنذار المســتخدم في الكشــف عن السرقات

المثبت على الباب يعتبر من النظم التقليدية لمتابعة المخاطر. ومن خلال استخدام التقارير الشبيهة بلوحة معلومات الإدارة أو غيرها من الآليات، يجب على المؤسسة أن تضع نظم متابعة للتحقق من الوضع الحالي للمخاطر الرئيسية المحددة وكذلك أجهزة إنذار الإشارة عند الحاجة إلى اتخاذ إجراءات تصحيحية. وعلى الرغم من عدم قيام أحد كبار المديرين ببناء أدوات المتابعة هذه أو تصميمها بوجه عام، فإن هذا المسئول التنفيذي نفسه ينبغي أن يكون في موقع يؤهله لطرح الأسئلة حول وضع أدوات متابعة مخاطر المؤسسة.

تعريفات إدارة المخاطر المؤسسية وأهدافها الصادرة عن لجنة المنظمات الراعية (COSO ERM): عرض محفظة المخاطر:

تحدثنا في الفصل الرابع من هذا الكتاب عن إطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية (COSO) وأهميته على أنه أداة لتقييم الضوابط الداخلية للمؤسسة وتعزيز حوكمة تقنية المعلومات. ويعد إطار إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية (COSO ERM) أداةً مماثلةً لهذا الإطار غير أنه يختلف عنه، فإطار المخاطر المؤسسية هذا من شأنه أن يساعد المؤسسات على أن تحتفظ بتعريف ثابت عن المقصود بالمخاطر على مستوى المؤسسة التي ينبغي أن تؤخذ بعين الاعتبار وبشكل متناسق عبر المؤسسة بأكملها. لقد قامت لجنة المنظمات الراعية (COSO) بإطلاق إطار إدارة المخاطر المؤسسية بطريقة مشابهة لإطار الرقابة الداخلية الخاصة بها والذي تم تطويره في وقت سابق. كما تم تشكيل مجلس استشاري يتكون من أعضاء من المؤسسات الراعية وتم التعاقد مع شركة برايس ووترهاوس كوبرز Pricewaterhouse Coopers (PWC) على تطوير وصف الإطار وصياغته. وقد تم نشر الوصف الخاص بالإطار عام ٢٠٠٤، والصفحات التالية من هذا الفصل تلخص مفاهيم إطار إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية. وعلى أية حال، فإننا ندعو القارئ أيضاً إلى الوصول إلى وصفٍ كاملٍ لإطار إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية. إذ يمكن تحميل نسخةٍ كاملة من إطار إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية أو شراؤها، وكذلك بعض المواد المختصرة الداعمة من خلال معهد المحاسبين القانونيين الأمريكيين (AICPA) أو موقع الويب الخاص بلجنة المنظمات الراعية من خلال الرابط التالي: www.coso.org

وكما بدأ إطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية باقتراح تعريف ثابت للموضـوع الذي يتناوله، يبدأ إطار إدارة المخاطر المؤسسـية أيضاً من خلال تعريف إدارة المخاطر المؤسسية على النحو التالي:

إن إدارة المخاطر المؤسسية هي عملية يقوم بها مجلس إدارة الكيان والإدارة وغيرهم من الموظفين، ويكون تطبيقها في شـكل إستراتيجية يتم وضعها في جميع أرجاء المؤسسة، وتكون مصممـة لتحديد الأحداث المحتملة التي قد تؤثر في الكيان، وكذلك تدير المخاطر لتكون في نطاق قدرة الكيان على تقبل المخاطر، وتقدم ضماناً معقولاً بتحقيق أهداف الكيان.

وحيث إن هذا هو تقريباً التعريف الأكاديمي، فإنه ربما يتعين على المرء النظر في النقاط الرئيسـية لإدارة المخاطر المؤسسية الصادرة عن لجنة المنظمات الراعية وتذكرها، والتي من ضمنها:

- **إدارة المخاطر المؤسسية عبارة عن عملية.** رغم أن تعبير "عملية" يُساء استخدامه غالباً، فإن القاموس يعرفها على أنها مجموعة من الإجراءات الرامية إلى تحقيق نتيجة. وفضلاً عن أن هذا التعريف لا يخدم العديد من المهنيين، فإن الفكرة هنا هي إدراك أن العملية ليسـت إجراءً ثابتاً مثل استخدام شـارة الموظف التي ما صُممت ولا طُبقت إلا للسماح فقط لأشخاص معينين لدخول أحد المرافق المؤمنة. فمثل هذا الإجراء الخاص بالشارة – الذي يعتبر بمثابة مفتاح القفل – ما هو إلا مجرد إجراء خاص بالسـماح أو عدم السماح بدخول شـخص ما إلى أحد المرافق. وتميل العملية إلى أن تكون ترتيباً أكثر مرونةً. ففي عمليـة اعتـماد الإقراض مثلاً، يتم وضـع قواعد قبول مع وجود خيـارات لتعديلها عند حـدوث اعتبارات أخرى. فالمؤسسـة هنا قد تلوي قواعد الإقـراض من أجل عميل غير مستحق للاقتراض يعاني من مشكلة على المدى القصير. فعملية إدارة المخاطر المؤسسية هي هذا النوع من العمليات. ولا تسـتطيع المؤسسة في كثيرٍ من الأحيان تحديد قواعد إدارة المخاطر من خلال كتاب قواعد صغير ومنظم بشـكل محكم. بل، ينبغي أن تكون هناك سلسلة من الخطوات الموثقة لمراجعة وتقييم المخاطر المحتملة واتخاذ الإجراءات المناسبة استناداً إلى مجموعة واسعة من العوامل الموجودة في جميع أرجاء المؤسسة.

- **يقوم أفراد يعملون في المؤسســة بتنفيذ عملية إدارة المخاطر المؤسسية.** لن تكون إدارة المخاطر المؤسســية فعالة إذا تم تنفيذها فقط من خلال مجموعة من القواعد التي يتم إرســالها لوحدة التشغيل من المركز الرئيسي للشركة، البعيد عن تلك الوحدات التشغيلية، حيث يوجد هؤلاء الأشــخاص العاملون بالشركة ممن قاموا بصياغة مسودة القواعد، وقد يكــون لديهم القليل من فهم العوامل المختلفة المحيطــة بهم التي يتم اتخاذ القرار بناءً عليها. ويجب أن يقوم على إدارة المخاطر أفرادٌ على مقربة كافية من مكان تلك المخاطر وحالها لفهم مختلف العوامل المحيطة بتلك المخاطر متضمناً ذلك آثارها.
- **يتم تطبيق إدارة المخاطر المؤسسية من خلال وضع إستراتيجيات عبر المؤسسة بالكامل.** تتعرض المؤسســات دائماً إلى إستراتيجيات بديلة متعلقة بمجموعة ضخمة من الإجراءات المســتقبلية المحتملة. فمثــلاً، هل يتوجب على الكيان أن يقتني أعــمالاً تكميليةً أخرى أم يكتفــي فقط ببنائها داخلياً؟ وهل ينبغي تبني تقنيــة جديدة في عمليات التصنيع أم الاكتفاء بالتمســك بالأســلوب المجرب والصحيح؟ إن الإدارة الفعالة للمخاطر المؤسسية يجب أن تلعب دوراً رئيســياً في وضع تلك الإســتراتيجيات البديلة. وبما أن هناك العديد من المؤسســات الكبيرة التي تحتوي عــلى العديد من وحدات التشــغيل المختلفة، فإنه ينبغي تطبيق إدارة المخاطر المؤسسية عبر تلك المؤسسة بأكملها باستخدام نوع من أنواع أساليب المحافظ الذي يقوم بدمج أنشطة المخاطر العالية والمنخفضة بعضها مع بعض.
- **يجــب الأخــذ في الاعتبار مفهــوم الرغبة في المخاطــر.** الرغبة في المخاطــرة هي مقدار المخاطرة، على المســتوى العام، الذي تكون المؤسســة ومديروها على استعداد لقبوله في سعيها لتحقيق القيمة المطلوبة. ويمكن قياس الرغبة في المخاطر من خلال الحس النوعي الذي يقوم على تصنيف المخاطر إلى فئات مثل عالية أو متوسط أو منخفضة؛ وبديلاً عن ذلك، يمكن تعريفها بطريقة نوعية. إن فهم الرغبة في المخاطر يغطي مجموعة واســعة من القضايا التي ســيتم مناقشــتها بمزيد من التفاصيل في الفصل العاشر من هذا الكتاب حــول مخاطر الحوكمة ومخاطر أمن تقنية المعلومات التي تمت الإشــارة إليها في فصول لاحقــة تدور حول تطبيق حوكمــة تقنية المعلومات. إن الفكرة الأساســية هنا هي أنه يجب أن يكون لدى كل مدير وكل مؤسســة عموماً مســتوى ما مــن الرغبة في المخاطر.

فالبعض سيقبل بالمشاريع المحفوفة بالمخاطر التي تبشر بتحقيق عوائد عالية، في حين يفضل البعض الآخر أكثر المشاريع المنخفضة المخاطر المضمونة العائد. كما يستطيع المرء أن يتصور هذا المفهوم الخاص بالرغبة في المخاطرة أو أن يقيسه على اثنين من المستثمرين الافتراضيين. فأحدهما قد يفضل سوق المال أو الصناديق ذات المؤشرات المنخفضة المخاطر جداً إلا أن عوائدها تكون عادة منخفضة، في حين قد يستثمر الآخر في أسهم شركات التقنية الصغيرة الناشئة.

- **توفر إدارة المخاطر المؤسسية ضماناً معقولاً فقط وليس إيجابياً حول إنجازات الأهداف.** والفكرة هنا تتضح في أن إدارة المخاطر المؤسسية، مهما كانت مدروسة أو مُنَفذة بشكل جيد، لا يمكن أن تمد الإدارة أو غيرها بأي ضمان مؤكد للنتائج. إن المؤسسة الخاضعة للرقابة بشكل جيد من خلال أشخاص على جميع المستويات تعمل باستمرار نحو تبني أهداف مفهومة وقابلة للتحقيق. وقد تتحقق تلك الأهداف فترة بعد فترة، حتى إن كان ذلك على مدى عدة سنوات. ومع ذلك، من الممكن أن يقع خطأ بشري غير مقصود أو سلوك غير متوقع من قبل آخرين، أو حتى وقوع كارثة طبيعية. فتسونامي[1] (موجات المد البحري العاتية) التي حدثت في المحيط الهندي في ديسمبر عام ٢٠٠٤ يعد مثالاً على تلك الأحداث غير المتوقعة. إذ سُجِّل أن آخر موجة تسونامي في هذا الجزء من العالم قد حدثت منذ نحو ٤٠٠ عام مضت. وعلى الرغم من تطبيق عملية إدارة مخاطر مؤسسية فعالة، فإن المؤسسة قد تتعرض لمثل هذا الإخفاق غير المتوقع بالمرة نتيجةً لتلك الأحداث غير المتوقعة، فالتأكيدات المعقولة لا توفر ضماناً مطلقاً.
- **تم تصميم إدارة المخاطر المؤسسية للمساعدة في تحقيق إنجاز الأهداف.** يجب أن تعمل المؤسسة، من خلال إدارتها، على وضع أهداف مشتركة عالية المستوى يمكن أن يتشارك فيها جميع أصحاب المصلحة. ومن أمثلة ذلك، كما وردت في وثائق إطار (COSO ERM)، أمورٌ مثل تحقيق السمعة الإيجابية والحفاظ عليها داخل مجتمعات الأعمال والمجتمعات الاستهلاكية للمؤسسة وتقديم تقارير مالية موثوقة لجميع أصحاب المصلحة والتزام المؤسسة بالقوانين واللوائح. إن البرنامج العام لإدارة المخاطر المؤسسية من شأنه أن يساعد المؤسسة على تحقيق تلك الأهداف.

وتكــون الأهــداف والغايات المتعلقة بإدارة المخاطر المؤسســية قليلة القيمة ما لم تكن منظمــة ومتناغمة معاً بطريقة تمكن الإدارة من أن تنظر في الجوانب المختلفة لهذه المهمة وأن تفهــم - نوعــا ما على الأقــل - الطريقة التــي تتفاعل بها بعضها مــع بعض على نحو متعــدد الأبعاد. هذه هي القوة الحقيقية لنموذج إطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية (COSO)؛ فهو يصف على سبيل المثال، كيف أن التزام المؤسسة بالقوانين واللوائح يمكن أن يؤثر في جميع مستويات الضوابط الداخلية، من عمليات المتابعة إلى بيئة الرقابة، وكيف أن هذا التوافق مهم لجميع كيانات المؤسسة أو وحداتها. وبطريقة مماثلة، قامت لجنة المنظمات الراعية (COSO) بتطوير نموذج إطار إدارة المخاطر المؤسسية الذي يوفر بعض التعريفات الشــائعة لإدارة المخاطر، والمســاعدة على تحقيق الأهداف الرئيسية للمخاطر في جميع أنحاء المؤسسة.

إطار إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية (COSO ERM):

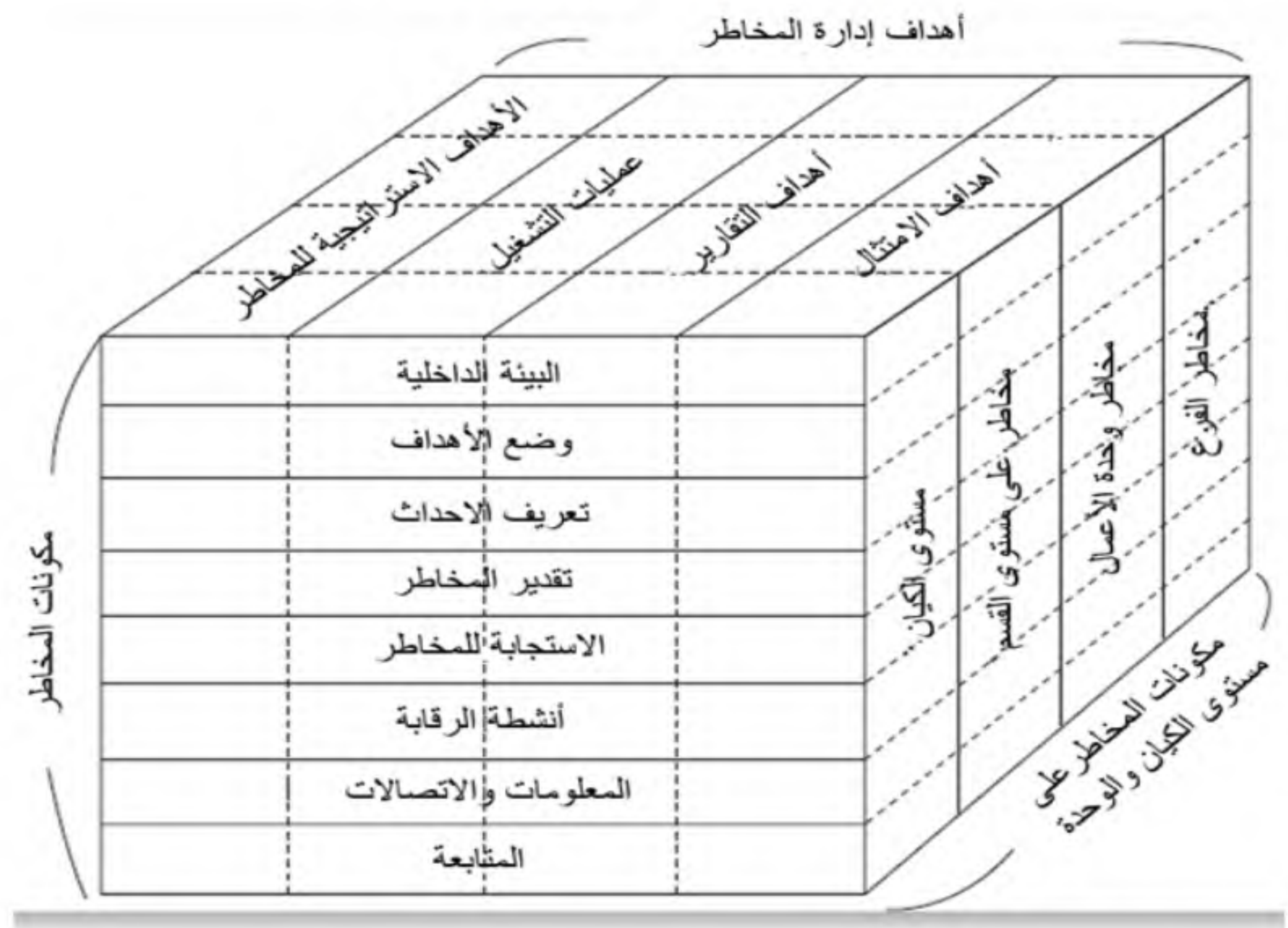
إن إطــار الرقابة الداخلية الصــادر عن لجنة المنظمات الراعيــة (COSO)، كما نوقش في الفصــل الرابع من هذا الكتاب، وتم وصفه في الشــكل التوضيحي (٤-١)؛ أصبح نموذجاً يحتــذى به في جميع أنحاء العالم، فهو يقــوم بعمل فعال جداً في وصف الضوابط الداخلية وتحديدها. وقد يبدو إطار (COSO ERM) من الوهلة الأولى مشــابهاً جداً لإطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية (COSO) ربما لأن بعض أعضاء الفريق نفسه قــد تم ضمهم إلى كل من مشروع الرقابة الداخلية ومشروع إدارة المخاطر المؤسســية. إن إطار (COSO ERM) كما هو موضح في الشــكل التوضيحي (٨-٤) عبارة عن مكعب ثلاثي الأبعاد يحتوي على المكونات التالية:

- أربعة أعمدة رأسية تمثل الأهداف الإستراتيجية للمخاطر المؤسسية.
- ثمانية صفوف أفقية وهي مكونات المخاطر.
- عدة مســتويات للمؤسسة، بدءاً من مستوى كيان "المقر الرئيسي" إلى مستوى الفروع الفردية. وتبعاً لنوع المؤسسة، قد توجد هنا "شرائح" كثيرة للنموذج.

يقوم هذا القسم بتسليط الضوء على بعض المكونات الأفقية لإطار (COSO ERM). كما يمكــن الحصول على وصف أكثر تفصيلاً لإدارة المخاطر المؤسســية الصادر عن لجنة المنظمات الراعية (COSO ERM) ومكوناته الثلاثية الأبعاد، وكيفية ارتباطها معاً من خلال زيارة الموقع www.coso.org ومن خلال الوصف الأكثر تفصيلاً لإدارة المخاطر المؤسســية الصادر عن لجنة المنظــمات الراعيــة (COSO ERM) المقدم من مؤلف هذا الكتــاب[٢]. كما يوفر إطار إدارة المخاطر المؤسسية (ERM) نموذجاً للمؤسسات لدراسة الأنشطة ذات الصلة بالمخاطر وفهمها على جميع مســتويات المؤسســة بالإضافــة إلى كيفية تأثير هذه الأنشــطة بعضها على بعض. وكجزء من فهم حوكمة تقنية المعلومات يهدف هذا الكتاب إلى مســاعدة كبار المديرين على فهم المخاطر التي تواجه مؤسساتهم وإدارتها على نحو أفضل.

شكل توضيحي (٨-٤)

إطارCOSO لإدارة المخاطر المؤسسية



يبدو أن هذا الوصف الخاص بإطار (COSO ERM) يشــبه إلى حد بعيد إطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية (COSO) الذي أصبح مألوفاً لدى العديد من

المهنيـين. فعندما تم إطلاق إطـار (COSO ERM) لأول مرة اعتقد البعض للوهلة الأولى اعتقاداً خاطئاً بأنه مجرد تحديث لإطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية (COSO) الأكثر شـيوعاً لديهم. فهذا الأمر قد يبدو خادعاً، فإطار (COSO ERM) لديه أهداف واستخدامات مختلفة! فهو ليس مجرد نسخة جديدة ومحسنة أو منقحة من إطار الرقابـة الداخلية الصادر عن لجنة المنظمات الراعيـة (COSO)، فهو أكثر من ذلك بكثير. وتلخـص الفقرات التالية هـذا الإطار من منظور تحديد مكونـات المخاطر ووضع أهداف إدارة المخاطـر. إن هدفنا هنا هو تقديم إطـار (COSO ERM) مع التركيز على الكيفية التي من خلالها يمكن أن تقوم إدارة المخاطر المؤسسية بتحسين الممارسات الخاصة بحوكمة تقنية المعلومات داخل المؤسسة.

مكونات إطار (COSO ERM): البيئة الداخلية:

كـما هو موضح في الشـكل التوضيحـي (٨-٤)، يوجد عنصر يسـمى البيئـة الداخلية وُضـع في الجزء العلوي من المكونات الخاصة بإطار (COSO ERM). وباسـتخدام بعض المصطلحـات القديمة، فإنه ينظر إلى البيئة الداخلية عـلى أنها بمثابة تتويج إطار (COSO ERM). فبالعـودة إلى العصر القديم حيث الجسـور المشـيدة من الطـوب، كان التتويج عبـارة عـن الحجر الذي يلحم معاً أقـواس الطوب التي ترتفع مـن كل جانب من جانبي الجسر لربط الجسر بأكمله معاً. ويشـبه مكون التتويج هذا أيضاً المربع الموجود في الجزء العلوي من الهيـكل التنظيمي، حيث يكون الرئيس التنفيـذي (CEO) هو الرئيس المعين لهذه الوظيفة. فهذا المستوى هو الذي يعد أساساً لجميع المكونات الأخرى في نموذج إدارة المخاطر المؤسسـية الخاص بالمؤسسة ويؤثر في الكيفية التي ينبغي أن يتم من خلالها وضع الإسـتراتيجيات والأهداف وكيفية هيكلة أنشـطة الأعمال المتعلقة بالمخاطر وكيفية تحديد المخاطر واتخاذ إجراءات بشـأنها. ويتكون هذا العنصر الذي يمثل الأسـاس الداخلي لإدارة المخاطر المؤسسية من العناصر التالية:

فلسـفة إدارة المخاطر: هي الاتجاهات والمعتقدات المشتركة التي تميز كيف أن المؤسسة تأخذ في الحسبان المخاطر في كل ما تفعله. وعلى الرغم من أن فلسفة إدارة المخاطر ليست في كثير من الأحيان أحد أنواع الرسـائل المنشـورة في مدونة قواعد السـلوك، فإنها تعد أحد

الاتجاهات التي من شـأنها السماح لكبار المديرين وغيرهم على جميع المستويات بالرد على اقتراح ما يخص المخاطر المرتفعة من خلال إجابة على غرار "لا، ليس هذا نوعاً من المشروعات التي تهتم به شركتنا". وبالطبع، فإن المؤسسـة التي تمتلك فلسـفة مختلفة خاصة بها قد ترد على هذا الاقتراح نفسه بإجابة على غرار، "تبدو مثيرة للاهتمام، ما معدل العائد المتوقع؟" في الحقيقة أن كلتا الإجابتين ليسـتا خاطئتين، لكن يجب على المنشـأة أن تحاول تطوير فلسفة واتجاه محدد ومتناغم حول التي تُقبل بها المشاريع المحفوفة بالمخاطر.

الرغبـة في المخاطر: مفهوم غير مألوف لدى كثير مـن المديرين، فالرغبة في المخاطر هي مقدار المخاطرة التي تكون المؤسسة مستعدة لقبولها في سعيها لتحقيق أهدافها. هذه الرغبة في المخاطـر يمكن قياسـها من حيث الكميـة أو النوعية، لكن ينبغي على جميع مسـتويات الإدارة أن يكون لديها فهمٌ عامٌ لهذا المفهوم وكذلك رغبة في المخاطر المؤسسية بكاملها.

مواقف مجلس الإدارة: لمجلس الإدارة دورٌ مهمٌ جداً في مراقبة بيئة المخاطر للمؤسسة. لذلـك يجب على المديرين المسـتقلين الخارجيين على وجه الخصـوص مراجعة الإجراءات الإدارية بعناية، وطرح الأسـئلة المناسـبة، فهـم يمثلون ضوابط الفحص والتوازن بالنسـبة للمؤسسـة. فعندما يكون أحد مسئولي المؤسسـة الكبار قوياً ولديه توجهٌ يقضي بأن "هذا لا يمكن أن يحدث هنا" عند النظر في المخاطر المحتملة المحيطة ببعض المسـاعي الجديدة، فإن أعضاء مجلس الإدارة يكونون غالباً هم أفضل من يطرح الأسـئلة الصعبة حول الكيفية المتعلقة برد فعل المؤسسة على حدث يقع ولم يكن من المتوقع حدوثه.

النزاهـة والقيم الأخلاقيـة: إن هذا العنصر من عناصر البيئـة الداخلية الخاص بإدارة المخاطر المؤسسـية (ERM) يحتاج إلى أكثر بكثير من مجرد مدونة قواعد سلوكية منشورة؛ بل إنه يدعو إلى نزاهة سـلوك أعضاء المؤسسة وقوة معاييرهم. لذا يلزم وجود ثقافة قوية للشركات لتقوم بتوجيه المؤسسـة، على جميع المستويات، في المساعدة على اتخاذ القرارات على أساس المخاطر المتعلقة بها.

الالتـزام بالكفاءة: تشـير الكفاءة إلى المعرفة والمهارات اللازمـة لإنجاز المهام المنوطة. والإدارة هـي التي تقرر الكيفية التي يتم بها إنجاز تلك المهام الحرجة المسـندة من خلال وضع إسـتراتيجيات مناسـبة وتعيين أفراد مناسـبين لأداء هذه المهام الإستراتيجية في أغلب

الأوقات. وقد رأينا جميعاً افتقار المؤسسات لهذا النوع من الالتزام. وتقوم الإدارة العليا بوضع الخطط الكبيرة والمدوية من أجل تحقيق هدف ما، إلا أنها غالباً لا تقوم ببذل أي جهد إيجابي من أجل تحقيق هذا الهدف. ويقوم سوق الأوراق المالية غالباً بفرض عقوبات على مثل هذه الأنشطة.

الهيكل التنظيمي: ينبغي أن يكون لدى الهيكل التنظيمي للمؤسسة خطوط واضحة للسلطة والمسئولية إلى جانب الخطوط الملائمة لتقديم التقارير. إن البنية الضعيفة للهيكل التنظيمي تجعل من الصعب القيام بتخطيط وتنفيذ ورقابة ومتابعة الأنشطة. وقد شهد المهنيون جميعهم الأوضاع التي لم تسمح فيها بنية المؤسسة بتكوين خطوط اتصال مناسبة.

تكليفات السلطة والمسئولية:

هذا التكليف هو المدى أو الدرجة التي وفقاً لها يتم تكليف مستويات أو شرائح من السلطة والمسئولية أو تفويضها لمجموعات وإدارات مختلفة في المؤسسة. إن الاتجاه السائد اليوم في العديد من المؤسسات هو دفع هذه الأمور مثل مستويات سلطات الموافقة إلى المستويات الدنيا من هيكل المؤسسة، وذلك بإعطاء موظفي الخط الأول التفويض وسلطة الموافقة بشكل أكبر. وثمة اتجاه ذو علاقة وهو "تسطيح" المؤسسات من خلال القضاء على مستويات الإدارة الوسطى. هذه الهياكل المؤسسية تعمل عادة على تعزيز إبداع الموظف وسرعة الاستجابة وزيادة رضا العملاء. وتحتاج هذه النوعية من المؤسسات التي تتعامل وجهاً لوجه مع العملاء إلى إجراءات قوية تحدد "القواعد" لجميع أعضاء طاقم العمل، فضلاً عن متابعة الإدارة المستمرة لهذه الإجراءات حيث يمكن إلغاء قرارات إذا لزم الأمر. كما ينبغي على جميع الأفراد في المؤسسة أن يعرفوا كيفية ترابط أعمالهم وأن يسهموا في تحقيق الأهداف العامة للمؤسسة.

المعايير الخاصة بالموارد البشرية: إن الممارسات التي تتبعها المؤسسة فيما يتعلق بتوظيف وتدريب وتعويض وترقية وتأديب الموظف، وجميع الإجراءات الأخرى، تبعث برسائل إلى جميع أعضاء المؤسسة بشأن ما هو مفضل أو ما هو مسموحٌ به أو ما هو ممنوع. وعندما تقوم الإدارة بغض الطرف عن بعض أنشطة "المنطقة الرمادية" بدلاً من اتخاذ موقف قوي حيالها، فإن هذه الرسالة تصل غالباً بسرعة إلى الآخرين في جميع أنحاء المؤسسة.

إن مكون البيئة الداخلية لإطار (COSO ERM) به اثنان من المخرجات الرئيسية التي تقوم بتغذية العناصر الأخرى في إطار (COSO ERM) وهما: فلسفة إدارة المخاطر في المؤسسة والرغبة النسبية في المخاطر. وبينما ناقشنا فلسفة إدارة المخاطر فيما يتعلق بمواقف مجلس الإدارة وسياسات الموارد البشرية، وأمور أخرى بينهما، فإن الرغبة في المخاطر يكون غالباً المقياس الأكثر مرونة عندما تقرر المؤسسة قبولها لبعض المخاطر ورفضها للبعض الآخر، وذلك تبعاً لاحتمالية حدوثها وتأثيرها. الشكل التوضيحي (٨-٥) يظهر خريطة الرغبة في المخاطر مما يدل على المدى الذي يتعين على المؤسسة وفقاً له قبول المخاطر تبعاً لاحتمالية حدوثها وتأثيرها. وتقول خريطة الرسم البياني هذه أن المؤسسة قد تكون على استعداد للانخراط في مشروع ذي تأثير سلبي عالٍ إذا كان هناك احتمالية منخفضة لحدوثه.

شكل توضيحي (٨-٥)

خريطة الرغبة في المخاطر



كما أن هناك بعداً ثالثاً لهذا المخطط وهو أن المؤسسة في بعض الأحيان يكون لديها رغبة أكبر نحو المساعي المحفوفة بالمخاطر إذا كان هناك إمكانية لتحقيق عائد أعلى.

مكونات إطار (COSO ERM): وضع الهدف:

تم إدراج هذ المكون أسـفل مكون البيئة الداخلية من حيث الترتيب، إذ يلخص مكون تحديـد الأهداف الخاص بإطار (COSO ERM) بعض الشروط الاسـتباقية الضرورية التي يلزم توافرها قبل أن تقوم الإدارة بوضع عملية فعالة لإدارة المخاطر في المؤسسة. وبالإضافة إلى البيئة الداخلية المذكورة سابقاً، ينبغي على المؤسسة وضع أهداف عالية المستوى تغطي الأنشطة الخاصة بعمليات التشغيل وإعداد التقارير والامتثال الخاصة بها.

ويدعو إطار (COSO ERM) إلى وضع بيان للمهمة (الرسـالة) وهو بيان عام ورسمي للأغراض التي يمكن أن تصبح اللبنة الأولى لتطوير إستراتيجيات وظيفية أكثر تحديداً ويصف غرض المنظمة وأهدافها ومواقفها العامة تجاه المخاطر. وإذا ما تم ذلك بشكل صحيح، فإن بيان المهمة (الرسـالة) سيساعد المؤسسة على تحديد سلسلة من أهداف عمليات التشغيل وتطويرها وتنفيذها ورفع تقارير بها وتحقيق مبدأ التوافق في هذا الشأن.

إن مكون البيئة الداخلية لإطار (COSO ERM) الذي سبق الحديث عنه، به اثنان من المخرجات الرئيسية هما: فهم فلسفة إدارة المخاطر في المؤسسة، وتقدير رغبة المؤسسة في المخاطر. هذان المخرجان يسـمحان لمكون تحديد الأهداف بتطوير سلسـلة من الأهداف للتقليل من المخاطر ولتعريف الرغبة في المخاطرة بشـكل رسـمي من حيث درجة تحمل المخاطر. ويقصد بدرجة تحمل المخاطر هنا الإرشادات أو المقاييس الرسمية التي يجب أن تسـتخدمها المؤسسة - على جميع المستويات - لتقدير ما إذا كانت ستقبل المخاطرة أم لا. إن وضع درجة تحمل المخاطر يمكن أن يكون صعباً للغاية بالنسـبة للمؤسسـات الرسمية. كما ستظهر مشـاكل إذا لم تكن القواعد الموضوعة محددة ومعرفة بشكل واضح ومفهومة جيداً ومطبقة بصرامة. وغالباً ما يكون من الصعب تطبيق القواعد، فعلى سـبيل المثال، في مـارس ٢٠٠٥، قـام مجلس إدارة شركة بإعفاء الرئيس التنفيذي للشركة من منصبه بسـبب "علاقـة عاطفية" مع موظفة[٣]. وكان يتم تجاهل هذا النوع من العلاقات غالباً في الماضي ولكـن تم الاعـتراف هنا باعتباره انتهاكاً لمدونة قواعد السـلوك، واتخـذ المجلس إجراءات سريعة وحاسمة حيال ذلك. فإذا كانت المؤسسة تريد إقامة مجموعة صارمة من القواعد، فإنه ينبغي إنفاذها في جميع أنحاء الكيان.

إن أفضل نهج يمكن للمؤسسة اتباعه هو وضع بعض النماذج المقبولة لدرجة تحمل المخاطر. وهذا يعني أنها قد تضع مدى مسموحاً به للمخاطر التي ستقبلها. فعلى سبيل المثال، تجد أن جميع المنتجات التي تأتي من خط الإنتاج قد يكون لها معدلات خطأ مقبولة ومحددة بشكل مسبق وتكون أقل من قيمة معينة. فخط الإنتاج في المؤسسة، على سبيل المثال، قد يرغب في إنتاج سلع بمعدل خطأ لا يزيد عن ٠,٠٠٥ في المئة. وهو معدل خطأ منخفض للغاية في العديد من المجالات، فإدارة الإنتاج في هذه الحالة ستقبل بمخاطر تخص أي مطالبات لضمان المنتج أو أي أضرار قد تلحق بسمعتها إذا وجدت أخطاء ضمن هذه الحدود الضيقة جداً. وبالطبع فإن نطاقات المخاطر في مؤسسة معنية بمنتجات الرعاية الصحية ستكون صارمة إلى أبعد حد.

إن الفكرة الأساسية هنا تتمثل في أنه يجب على المؤسسة أن تحدد إستراتيجياتها وأهدافها المتعلقة بالمخاطر، وفي ظل الإرشادات، يجب أن تقرر المؤسسة مدى رغبتها وتحملها للمخاطر. بمعنى، ما مستوى المخاطر التي تكون المؤسسة على استعداد أن تقبله، وبافتراض وجود تلك القواعد الخاصة بقبول المخاطر، فما هو المقدار الذي تكون على استعداد أن تحيد عنه فيما يخص هذه المقاييس المحددة بشكل مسبق؟ الشكل التوضيحي (٨-٦) يلخص العلاقة بين هذه المكونات الخاصة بتحديد أهداف إطار (COSO ERM) التي يمكن استخدامها لمؤسسة تصنيع متوسطة الحجم. فبدءاً من المهمه الشاملة، يكون النهج عبارة عن (١) وضع الأهداف الإستراتيجية لدعم إنجاز تلك المهمة (٢) وضع إستراتيجية لتحقيق الأهداف (٣) تحديد أي أهداف ذات علاقة و(٤) تحديد الرغبات في المخاطر لاستكمال تلك الإستراتيجية. وقد تم تبني هذا المخطط من المواد الإرشادية المنشورة الخاصة بإطار (COSO ERM)[٤]. ومن أجل إدارة المخاطر على جميع المستويات ومراقبتها، تحتاج المؤسسة إلى تحديد أهدافها وتحديد مدى تحملها للمخاطر عندما تضطر للانخراط في ممارسات محفوفة بالمخاطر ومدى تمسكها بهذه القواعد. ولن تسير الأمور بالشكل السليم إذا ما قامت المؤسسة فقط بتحديد بعض الأهداف المتعلقة بالمخاطر وبعد ذلك تستمر في تجاهلها.

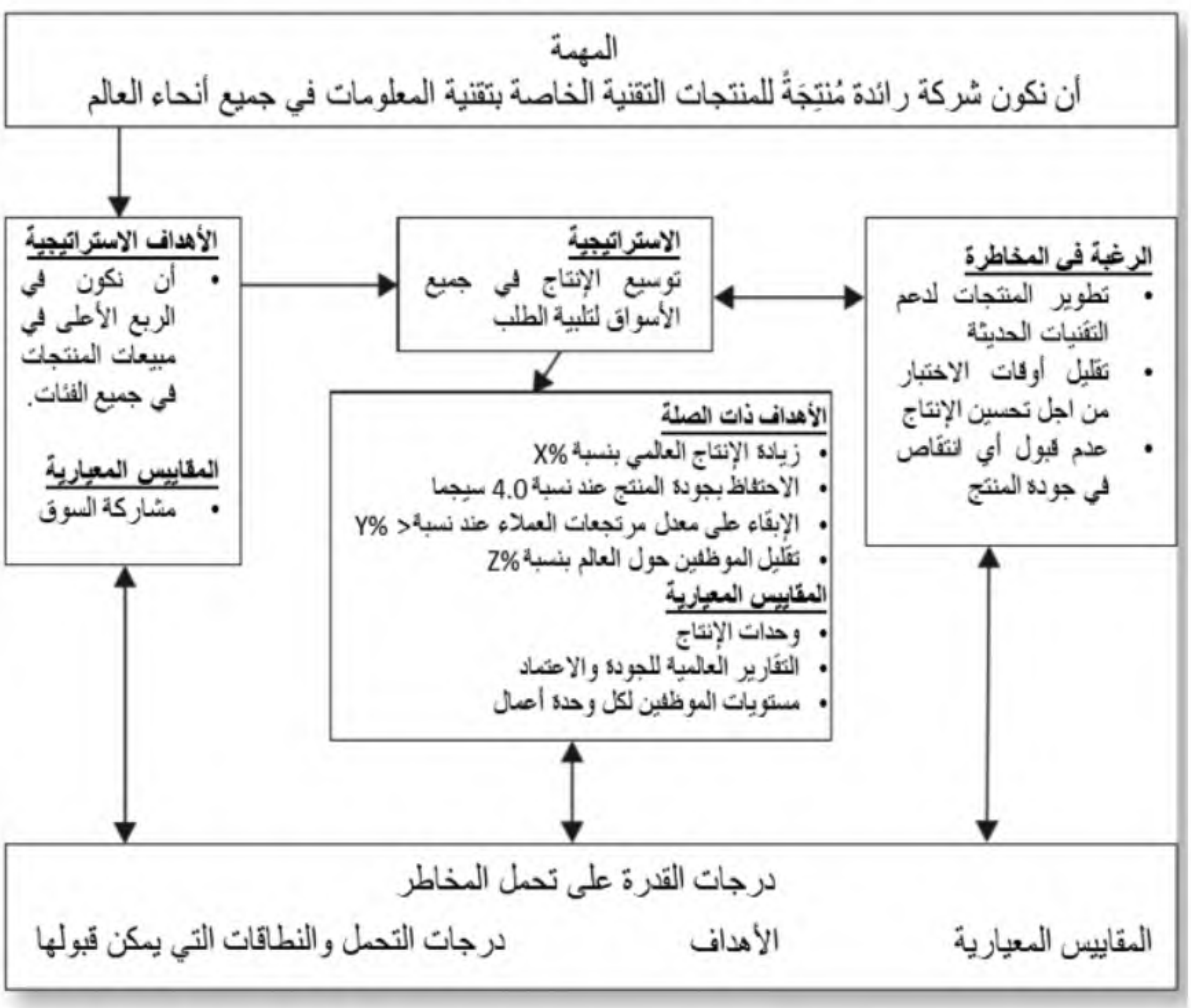
مكونات إطار (COSO ERM): تحديد الحدث:

يقصد بالأحداث الحوادث أو الوقائع الداخلية أو الخارجية في المؤسسة التي تؤثر في تنفيذ إستراتيجية إدارة المخاطر المؤسسية أو تحقيق أهدافها. وبينما يكون الاتجاه السائد

هو التفكير في مثل هذه الأحداث بشــكل ســلبي (تحديد الخطأ الذي حدث)، فإنه يمكن أن تكون إيجابية أو ســلبية أو كليهما. وبالرغم من أن العديد من المؤسســات اليوم تشهد مســتوىً قوياً من متابعة الأداء، فإن عملية المتابعة تلك تميل إلى التركيز على مســائل مثل التكاليف والميزانيات وضمان الجودة والامتثال وما شابه ذلك. إن أهداف المخاطر الخاصة بإدارة المخاطر المؤسسية التي سبق الحديث عنها يمكن أن تصبح مفقودة في هذه العملية التــي تختص بمتابعــة المزيد من الأهداف التشــغيلية والأهداف التشــغيلية الموجهة نحو العملية بشكل أكبر. وتُطَبِق المؤسسات في العادة عمليات قوية لمتابعة مثل هذه الأحداث كالتباينات الملائمة في الميزانية وغير الملائمة على وجه الخصوص.

شكل توضيحي (٨-٦)

مكونات وضع أهداف المخاطر في COSO ERM



ومع ذلك ففي كثير من الأحيان لا تكون هناك متابعة منتظمة، سواء للأحداث الفعلية أم للعوامــل المؤثرة التي تعد الدافــع وراء مثل هذه الأحداث الخاصــة بتقلبات الميزانية. وتشمل بعض العوامل المؤثرة التي ينبغي أن تكون جزءاً من عنصر تحديد الأحداث فى إطار (COSO ERM) ما يلي:

- **الأحــداث الاقتصاديــة الخارجية:** قد تؤثر الاتجاهات الجاريــة، قصيرة كانت أم طويلة الأجل، في بعض عناصر الأهداف الإستراتيجية للمؤسسة، ومن ثم يكون لها تأثير في الإطار العام لإدارة المخاطر المؤسسية. ومثال على ذلك الحدث الاقتصادي الخارجي الذي وقع في ٦ مايو ٢٠١٠ والذي شــهدت فيه أســواق الأســهم الأمريكية والعالمية خسائر فادحة فيما كان يعرف باسم الانهيار السريع (Flash Crash)[٥]. وقد استردت الأسواق عافيتها بسرعة، إلا أن الحدث قد تسبب في قيام العديد باتخاذ إجراءات علاجية متسرعة وكانت غالباً غير مدروســة بشــكلٍ جيد. وقد كان هذا الحدث الاقتصادي الخارجي غير متوقع بالمرة.
- **الكــوارث البيئيــة الطبيعية:** إن العديد مــن الأحداث، مثل الحرائــق أو الفيضانات أو الزلازل، يمكن أن تصبح حوادث أثناء تحديد المخاطر الخاصة بإدارة المخاطر المؤسســية. ويمكن أن تشــمل الآثار هنا فقدان إمكانية الوصول إلى بعض المواد الخام الرئيســية، أو أضراراً جسيمة يمكن أن تلحق بالمرافق المادية أو عدم توفر الموظفين.
- **الأحداث السياســية:** قد ينتج عن القوانين واللوائح الجديــدة وكذلك نتائج الانتخابات، مخاطر مؤثرة يكون لها تأثيرات ذات صلة بالمخاطرعلى المؤسســات. ويكون لدى العديد من المؤسســات الكبيرة إدارة خاصة بالشــئون الحكومية تســتعرض التطورات والمساعي المبذولــة لإجــراء التغييرات. ومع ذلــك، فإن مثل هذه الإدارات قــد لا تتماشى دائماً مع أهداف إدارة المخاطر المؤسسية.
- **العوامل الاجتماعية:** بينما يكون حدث خارجي مثل الزلزال مفاجئاً ويحدث دون ســابق إنذار، فإننا نجد أن معظم التغيرات الخاصة بالعوامل الاجتماعية تكون عبارة عن أحداث تتطور ببطء. وتشمل هذه الأحداث التغيرات الديموغرافية والأعراف الاجتماعية وغيرها من الأحداث التي قد تؤثر في المؤســســات وعملائها مع مرور الوقت. ومثال على التغيير

المجتمعي واقعة الإقالة تلك التي تمت الإشارة إليها سابقاً للرئيس التنفيذي للشركة بسبب علاقــة غير شرعية تمت بالتراضي مع موظفة أخرى بالشركة ربما تم تجاهلها لو حدثت في عصر آخر. إلا أن تغير العادات الاجتماعية اليوم هو الذي أدى إلى تلك الإقالة.

- **أحــداث البنية التحتيــة الداخلية:** في كثير من الأحيان تقوم المؤسســات بإجراء تغيرات حميــدة من شــأنها أن تؤدي إلى أحداث أخــرى متعلقة بالمخاطر. فعلى ســبيل المثال، التغير في إجراءات خدمة العملاء يمكن أن يسبب شكاوى كبرى وانخفاضاً في رضا العملاء. فالطلــب الشــديد والمتصاعد على منتج جديد من قبل العمــلاء قد يؤدي إلى تغيرات في متطلبات الطاقة الاستيعابية للمصنع والحاجة إلى المزيد من الموظفين.
- **الأحــداث المتعلقة بالعمليات الداخلية:** على غرار أحداث البنية التحتية يمكن أن تؤدي التغيرات في العمليات الرئيســية إلى وقوع مجموعة كبيرة من الأحداث المتعلقة بتحديد المخاطر. وكما هو الحال بالنســبة للعديد من هــذه العناصر، فإن تحديد المخاطر قد لا يكــون فورياً، وقد يمر بعض الوقت قبل أن تشــير الأحداث المتعلقة بالعملية إلى الحاجة إلى تحديد المخاطر.
- **الأحــداث التقنيــة الخارجية والداخليــة:** تواجه جميع المؤسســات الكثير من الأحداث التقنية المتواصلة التي يمكن أن تؤدي إلى الحاجة إلى تحديد رسمي للمخاطر، فبعضها يتم تدريجياً مع مرور الوقت في حين أن البعض الآخر يكون مفاجئاً بشــكل كبير. فقد كانت الشــبكة العنكبوتية العالمية لوقت ما قيد اســتخدامنا، إلا أن التحــول إلى بيئة الإنترنت بالنســبة للكثيرين تم بشكل تدريجي إلى حد ما. وفي حالات أخرى، فإن التوسع في نظم حوسبة الشبكات الاجتماعية التي تم الحديث عنها في الفصل الحادي والعشرين من هذا الكتــاب كان له تأثير كبير في المؤسســات من حيث العلاقات مــع أصحاب المصلحة لدى المؤسسة وسمعتهم.

تحتاج أي مؤسسة إلى تعريف واضح لما تراه عبارة عن أحداث هامة للمخاطر، ومن ثم يجــب أن يكون لديها عمليات مطبقة لمتابعة كل أحداث المخاطر الهامة المحتملة المتنوعة تلك، وعلى هذا يمكن للمؤسسة أن تتخذ الإجراءات المناسبة. وفي الواقع يعد هذا أحد أنواع التفكير الواعد لعملية تكون غالباً صعبة الإدراك داخل العديد من المؤسسات.

إن عمليــة النظــر في مختلف الأحداث الداخلية والخارجيــة المحتملة للمخاطر واتخاذ قــرار بشــأن أي من هذه الأحداث يتطلب مزيداً من الاهتمام وقــد يكون أمراً صعباً، لكن إطار (COSO ERM) يقدم هنا بعض المساعدة فهو يقترح أن تقوم المؤسسة بوضع بعض العمليات الرســمية لمراجعة المخاطــر الهامة المحتملة ومن ثم تبــدأ عملية اتخاذ الإجراء. وتبعاً لإرشــادات إطار (COSO ERM)، فإن المؤسســة قد تأخذ بعــين الاعتبار بعضاً من الأساليب التالية:

- **مستودعات الأحداث:** ينبغي على إدارة المؤسسة أن تراجع الأحداث الأخرى المتعلقة بالمخاطر الشــائع حدوثها في الصناعة أو في مجال وظيفي معين لإحدى المؤسســات. بمعنى أنه يجب على المؤسسة أن تنظر في إنشاء أرشيف مصدري لـ "الدروس المستفادة". ويعد هذا نوعاً من أنــواع البيانات التاريخية التي تم الحصول عليها عن طريق أعضاء في المؤسســة طالت مدد بقائهــم فيها، ويمكنهم تقديم أنواع من التعليقات مثل "لقد جربنا ذلك منذ عدة ســنوات، ولكــن ...". إن هذا النــوع من التأريخ في كثير من الأحيان يكون غير موجود في مؤسســات اليوم، غير أن الإدارة الفعالة لإدارة المخاطر يمكن أن توفر بعض المساعدة في هذا المقام.
- **ورش العمل الميسرة:** يمكن للمؤسســة أن تعقد ورش عمل للعديد من الإدارات لتناقش بدايــةً العوامل المحتملــة للمخاطر التي يمكــن أن تكون نتيجة للأحــداث الداخلية أو الخارجيــة المتنوعة ومن ثم تقوم بتطوير خطط عمــل لتصحيح المخاطر المحتملة. يعد هــذا أحد الأســاليب المقترحة التي تبــدو جيدة، لكن جرت العادة بالنســبة للعديد من المؤسسات أنها لا تقوم بتخصيص جزء من أوقاتها الثمينة لمقابلة مجموعات من مختلف الإدارات للحديث عن المخاطر باستخدام صيغة من نوع "ماذا سيحدث لو .."
- **مقابلات واســتبيانات واستطلاعات:** إن المعلومات التي تخص أحداث المخاطر المحتملة يمكن أن تأتي من مجموعة واسعة من المصادر. مثل التعليقات على خطابات رضا العملاء، والتعليقات التي تأتي من نظم وســائل التواصل الاجتماعــي. أو التعليقات الصادرة من المقابلات النهائية مع الموظفين التاركين لوظائفهم. وهناك حاجة للحصول على المعلومات وتصنيفها من أجل تحديد أي منها يمكن اعتباره مؤشراً على وجود أحداث مخاطر. وهذه الأنواع من الردود ستساعد على بناء ثقافة إدارة المخاطر المؤسسية.

• **تحليل تدفق أو ســير العمليات:** إن المواد الخاصة بدعم تقنيات تطبيق إطار (COSO ERM) توصي باستخدام مخططات التدفق لمراجعة العمليات وتحديد الأحداث المحتملة للمخاطر، وبالنســبة للعديد من المؤسسات فإن مخططات تدفق العملية تتشابه إلى حد بعيد مع وثائق الرقابة الداخليــة التي كان ينبغي إعدادها وتحديثها باعتبارها جزءاً من أعمال التوثيق الخاصة بالبند ٤٠٤ من قوانين ســاربينز- أوكسلي SOx، حيث يتم تحديد الضوابــط الداخلية وأي نقطة من نقاط الضعــف الموجودة في العملية الرقابية. وقد تم مناقشة هذه العمليات في الفصل الثاني من هذا الكتاب الخاص بقانون ساربينز أوكسلي.

• **الأحداث الرائدة ومحفزات التصعيد:** يجب على إدارة المؤسســة أن تقوم بوضع سلسلة من الأهداف الخاصة بوحدة الأعمال، ولا شــك أن معايــير القياس ضرورية لتحقيق تلك الأهــداف، فمعايير درجة تحمل المخاطر تكون ضرورية لتعزيــز الإجراءات التصحيحية. فعلى سبيل المثال، قد تقوم مجموعة تقنية المعلومات في المؤسسة بوضع هدف للحفاظ على الضوابط الأمنية المعززة بشأن التهديدات الهجومية لاختراق شبكة تقنية المعلومات. وبقيــاس عدد محاولات الاقتحام التــي تم تحديدها خلال فترة معينــة، وجدنا أن عتبة threshold ذلك تجاوزت ربما ثلاث تدخلات في شــهر معين، مما أدى إلى اتخاذ مزيد من الإجــراءات. وتوجد اليوم أدوات برمجية جيدة جداً متاحة تســمى لوحات المعلومات[٦] dashboards لمتابعة الأداء الخاص بجوانب المؤسســة، وفي الغالب تكون معقدة للغاية. هذه التطبيقات تعمل على نحو يماثل عمل التحكم على لوحة العدادات في الســيارة، إذ إن المؤشرات تعطي إشارات ضوئية في ظروف معينة مثل انخفاض ضغط الزيت أو ارتفاع درجة حرارة المحرك. والفكرة هي أن يُقدم تقريرٌ عن حالة المخاطر من خلال رســومات بســيطة، سهلة الفهم إلى حد ما مثل الأسهم العلوية أو السفلية أو شعارات إشارة المرور الشائعة الحمراء والصفراء والخضراء.

• **تتبع بيانات أحداث الخسارة:** في حين أن أسلوب لوحة المعلومات يقدم فقط متابعات لأحــداث المخاطر وقت حدوثها، فإنه يكــون من المفيد غالباً وضع الأمور في نصابها بعد مرور بعض الوقت. ويشــير تتبع حادث الخســارة إلى اســتخدام كل من مصادر قاعدة البيانات الداخلية والعامة لتتبع النشاط في المجالات ذات الاهتمام. ويمكن لهذه المصادر

أن تغطي مجموعة واسعة من المجالات بدءاً من قيادة المؤشرات الاقتصادية إلى أن تصل إلى معدلات فشـــل المعدات الداخلية. ومرة أخرى، يجب على المنشـــأة تثبيت عمليات فعالـــة لتحديد المخاطر بهـــدف تتبع كل من الأحـــداث الداخليـــة والخارجية المتعلقة بالمخاطر.

إن أدوات وأســـاليب تحديد المخاطر التي تمت مناقشتها للتو يمكن أن تسفر عن بعض المعلومات القيمة جداً والمفيدة للمؤسســـة، والتي تحدد إما المخاطر وإما الفرص أو الاثنين معـــاً. إن الحل يكمن في الحاجة إلى تحليلات جيـــدة للبيانات، فضلاً عن الشروع في خطط عمل، سواء للحماية من المخاطر أو للاستفادة من الفرص المحتملة.

مكونات إطار (COSO ERM): تقييم المخاطر:

تحدثنا عن مكون البيئة الداخلية باعتباره تتويجاً أو حجر زاوية لإطار (COSO ERM)، مع مكون المتابعة باعتباره عنصراً أساســـياً لدعم الإطار. ويقع عنصر تقييم المخاطر تقريباً في وســـط الإطار ويمثل جوهر إطار (COSO ERM). كما يســـمح مكـــون تقييم المخاطر للمؤسسة بالنظر في الأثر المحتمل للأحداث المرتبطة بالمخاطر المحتملة على إنجاز المؤسسة لأهدافهـــا. ويجب تقييم هذه المخاطـــر من منظورين: احتمالية حدوث المخاطر، وتأثيرها المحتمـــل. وكجزء أســـاسي لعملية تقييم المخاطر هذه، تحتـــاج الإدارة أيضاً إلى أن تنظر في مفهومين أساسيين: المخاطر المتأصلة والمخاطر المتبقية.

١- **المخاطـــر المتأصلة (الكامنة):** كما حددهـــا مكتب الحكومة الأمريكية للإدارة والميزانية، فإن المخاطر المتأصلة هي "إمكانية هدر أو فقدان أو استخدام غير مصرح به أو اختلاس أو اســـتغلال بسبب طبيعة النشـــاط نفسه". والعوامل الرئيســـية التي تؤثر في المخاطر المتأصلة في أي نشـــاط داخل الشركة هي حجـــم ميزانيته وقوة إدارة المجموعة وحنكتها وببساطة الطبيعة الأصيلة لأنشطتها. وتكون المخاطر المتأصلة خارجة عن سيطرة الإدارة ونابعة عادة من العوامل الخارجية. فعلى ســـبيل المثال، متاجر التجزئة الرئيســـية وول مارت Walmart كبيرة جداً ومهيمنة على أســـواقها ويواجهها مستوى معين من مختلف المخاطر المتأصلة بسبب حجمها الهائل.

٢- المخاطر المتبقية: هي تلك المخاطر التي تبقى بعد اســتجابة الإدارة لتهديدات المخاطر وتطبيق الإجراءات المضادة. ويوجد دائماً مستوى ما من المخاطر المتبقية.

يدل هذان المفهومان على أن إدارة المؤسسة ستواجه دائماً بعض المخاطر. فبعد أن تقوم المؤسسة بمعالجة المخاطر التي خرجت من عملية تحديد المخاطر، فإنها تظل تواجه بعض المخاطر المتبقية التي يلزم علاجها لاحقاً، كالعديد من المخاطر المتأصلة القليلة التـأثير. وول مارت، على سبيل المثال، يمكن أن تتخذ بعض الخطوات للحد من المخاطر المتأصلة المتعلقة بهيمنة الســوق. لكنها لا يمكن أن تفعل شــيئاً أساســياً بشــأن المخاطر المتأصلة (الكامنة) لزلزال طبيعي كبير في منطقة عمليات التشغيل.

إن الاحتماليــة والتأثــير هما أيضاً مكونان رئيســيان آخران ضروريــان لتقييم المخاطر. فالاحتماليــة هي إمكانية حدوث مخاطرة ما، وتوصف غالباً بأنها احتمال مرتفع أو احتمال متوســط أو احتمال منخفض للمخاطر التي تحدث. وتوجد بعض الأدوات الكمية الجيدة هنــا كذلك، لكنها غير مجدية كثيراً في تقدير احتماليــة حدوث المخاطرة من حيث العلامة العشرية المتعددة إذا لم يكن هناك أي أســاس لتطويــر ذلك العدد الدقيق إلى ما هو أبعد من الحسابات الإحصائية الاعتيادية.

إن تقديــر التأثــير في حالة حدوث المخاطرة يعتبر أســهل بعض الــشيء. فيمكن أن تقوم المؤسســة بوضع بعض التقديرات الدقيقة نســبياً لأمور مثل تكلفة استبدال المرافق والمعدات، تكلفة اســتعادة نظام معين، وإلى حــد ما تكلفة الفرص التجاريــة الضائعة (الأعمال الخاسرة) بسبب العطل. وعلى كل حال، فإن المفهوم الشامل وراء إدارة المخاطر المؤسسية (ERM) ليس تطوير حســابات دقيقة وحسابات على المســتوى الاكتواري فيما يخص المخاطر لكن للحصول عــلى مقياس معين لتوفير إطــار فعال لإدارة المخاطر. ويمكن تطوير تحليل احتماليات المخاطر والتأثيرات المحتملة من خلال سلســلة من المقاييس النوعية والكمية. فالفكرة الأساســية هي تقييم جميع المخاطر التي تم تحديدها وتصنيفها من حيث الاحتمالية والتأثير بطريقة متناغمة.

مكونات إطار (COSO ERM): الاستجابة للمخاطر:

إن الخطوة التالية بعــد تقييم المزيد من المخاطر الهامة وتحديدها، هي تحديد كيفية الاســتجابة لمختلف هذه المخاطر التي تم تحديدها. وتعد هذه من المســئوليات الإدارية،

فالإدارة هي التي تقوم بإجراء مراجعة دقيقة لاحتمالات المخاطر المقدرة وتأثيراتها المحتملة، كما أنها تأخذ في الاعتبار التكاليف والفوائد المرتبطة بها. ولوضع إستراتيجيات ملائمة للاستجابة للمخاطر يتم اتباع أي أسلوب من الأساليب الأربعة الأساسية:

١- **التفادي (التجنب):** إستراتيجية تعتمد البعد عن المخاطر، مثل بيع أحد وحدات الأعمال التي يمكن أن تؤدي إلى مخاطرة أو الخروج من منطقة جغرافية محل قلق. وتكمن صعوبة تطبيق هذه الإستراتيجية في أن المؤسسات في كثير من الأحيان لا تتخلى عن المنتج أو تبتعد عن المخاطر إلا بعد أن يقع الحدث الخاص بالمخاطرة. فإذا لم تكن هناك رغبة في المخاطر حتى وإن كانت منخفضة للغاية، فمن الصعب الابتعاد عن منطقة العمل أو خط الإنتاج بسبب ظهور مخاطر محتملة في المستقبل، هذا إذا ما كان كل شيء في الوقت الحاضر يسير على ما يرام في نواحٍ أخرى. وقد تكون إستراتيجية التفادي مكلفة إذا كانت الاستثمارات قد اعتُمدت للدخول في منطقة مرتبطة بحدوث انسحاب تبعي لتجنب المخاطر.

٢- **التخفيف:** قد تكون قرارات الأعمال قادرة على الحد من مخاطر معينة. فتنويع المنتجات قد يقلل من مخاطر الاعتماد القوي للغاية على خط إنتاج واحد رئيسي. كما أن تقسيم مركز عمليات تشغيل تقنية المعلومات إلى موقعين منفصلين جغرافياً سيقلل من مخاطر بعض الأعطال الكارثية. وتوجد مجموعة واسعة من الإستراتيجيات الفعالة في كثير من الأحيان للحد من المخاطر على جميع المستويات التي تنزل بها إلى المرحلة الدنيا، لكنها تكون مهمة من الناحية العملية لموظفي التدريب المتعدد التخصصات.

٣- **المشاركة:** تتقاسم جميع المؤسسات تقريباً وكذلك الأفراد بصورة منتظمة بعض مخاطرها من خلال شراء التأمين لتطويق تلك المخاطر أو مشاركتها. وهناك العديد من التقنيات الأخرى المتوفرة هنا كذلك. فبالنسبة للمعاملات المالية، فإن المؤسسة يمكن أن تنخرط في العمليات التحوطية للحماية من تقلبات الأسعار المحتملة. ومن الأمثلة الشائعة على التطويق هو استخدام المستثمر لخيارات البيع أو الطلب لتغطية التحركات القوية للأسعار. كما يمكن مشاركة المخاطر والمزايا المحتملة للأعمال من خلال اتفاقيات مشتركة.

٤- **القبول:** ويقصد بها إســتراتيجية اللاإجراء. فمثلاً عندما يكون لدى المؤسســة "تأمين ذاتي" ضد بعض المخاطر، فبدلاً من شراء وثيقة تأمين في الأســاس، يجب على المؤسسة أن تنظــر في احتمالية المخاطرة وأثرها في ضوء تحمــل المخاطر الموضوعة، وبعد ذلك تقرر ما إذا كانت ســتقبل هذه المخاطرة أم لا. ونظــراً لكثرة المخاطر وتنوعها، يمكن أن يكون هذا هو نهج المؤسســة، فالقبول غالباً ما يشــكل إســتراتيجية ملائمة لبعض المخاطر.

وينبغي على الإدارة وضع إســتراتيجية عامة للاســتجابة لــكل مخاطرة من مخاطرها باســتخدام نهج قائم على أحد هذه الإســتراتيجيات الأربع العامة. وللقيام بذلك، ينبغي النظر في التكاليف مقابل الفوائد الناتجة عن كل اســتجابة للمخاطر المحتملة لمواءمتها بشــكل أفضل مع الرغبة في المخاطر الإجمالية للمؤسســة. فمثلاً، إدراك المؤسســة بأن تأثير مخاطرة معينة يكون منخفضاً نســبياً ســيتم موازنته مقابل درجة تحمل منخفضة للمخاطــرة، وهذا يشــير بدوره إلى أن التأمــين يجب شراؤه لتوفير الاســتجابة للمخاطر المحتملة. وبالنسبة لكثير من المخاطر، فإن الاستجابات المناسبة تكون واضحة ومفهومة تقريباً للجميع. فعملية تشــغيل تقنية المعلومات، على سبيل المثال. ينبغي أن تستهلك الوقت والموارد لإجراء نســخ احتياطية لملفات البيانات الرئيسية وتنفيذ خطة استمرارية العمل.

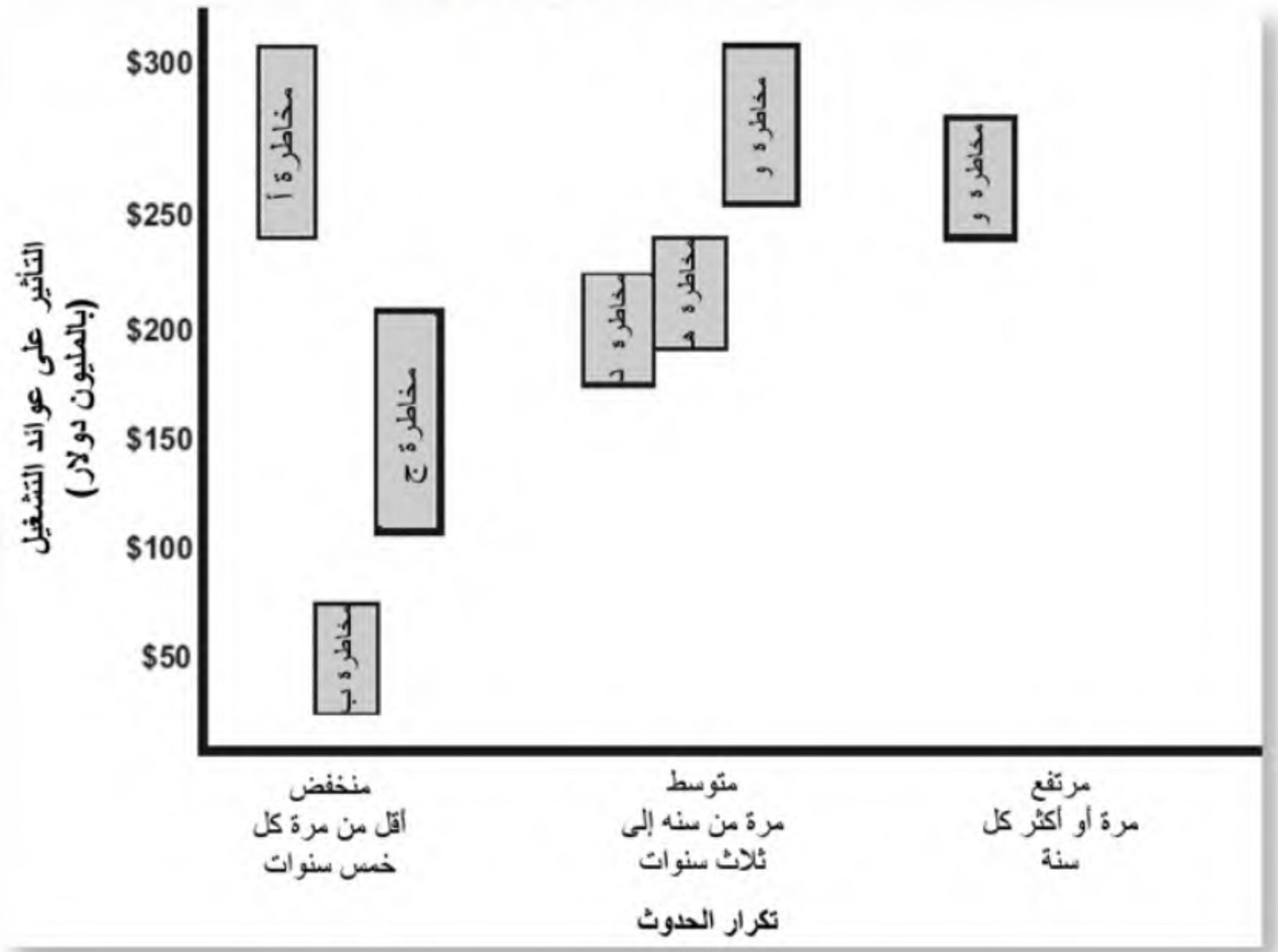
إن المؤسســة، عنــد هذه النقطــة، يجب أن تعــود إلى الأهداف العديــدة للمخاطر التي تــم وضعها وكذلك نطاقــات تحمل تلك الأهداف. ومن ثم ينبغي أن تعيد مناقشــة كل من الاحتمالية والتأثير المرتبطين بكل مخاطرة من المخاطر التي تم تحديدها ضمن أهداف المخاطر تلك لوضع تقييم لكل من هذين الصنفين للمخاطر. كما يلزم إجراء تقييم شــامل لاستجابات المخاطر المخطط لها وكيفية مواءمة تلك المخاطر مع درجات التحمل الكلية لمخاطر المؤسسة. وعنــد هذه النقطة في عملية تقييم المخاطر، يتعين على المؤسســة أن تُقيِّم الاحتمالية والتأثير المحتمــل لكل من المخاطر المحيطــة بأهدافها، وكذلك بعض التقديرات لــكل منهما. وتقوم بالخطــوة التالية المتمثلة في تطوير مجموعة من اســتجابات المخاطــر المحتملة. ولعل هذه هــي أصعب خطوة في بناء إطار برنامج فعال لإطار (COSO ERM). فمن الســهل نســبياً

تحديد خمســة في المئة مــن احتمالية مخاطر وقوع حريق في حاويــة نفايات، ومن ثم وضع الخطوط العريضة للاســتجابة للمخاطر كتثبيت طفاية حريق في مكان قريب. ومع ذلك، فإن الاســتجابات لمعظم المخاطر تكون أكثر تعقيداً وتتطلب خططاً تفصيلية إلى حد ما للاستجابة للمخاطر.

ويجب على المؤسسة في البداية استعراض جميع مخاطرها الرئيسية المحددة ذات التأثير العالي والاحتمالية العالية ووضع سلســلة من خطط الاســتجابة للمخاطر. وعلى أية حال، قــد تكون هذه عملية إدارية صعبة. وعلى الرغم من أنها قد تكون ســهلة نســبياً، كاتباع مثالنــا الســابق، الخاص بتثبيت طفاية حريــق لتوفير الحماية من حرائــق حاوية نفايات، فــإن الأمــور لا تكــون عادة بهذه البســاطة. والنقطة الأساســية هنا تتضــح في أن عملية تطوير عمليات الاســتجابة للمخاطر في حد ذاتها تتطلب قدراً كبيراً من التخطيط والتفكير الإســتراتيجي. إن البدائل العديدة والمختلفة للاســتجابة للمخاطــر تنطوي على التكاليف والوقــت والتخطيط التفصيــلي للمشروع. وبالإضافة إلى التخطيط والتفكير الإســتراتيجي، فإن هــذه العملية الخاصة بتخطيط الاســتجابة للمخاطر تتطلب مســاهمة إدارية كبيرة والموافقة على التعرف على مختلف الاستجابات البديلة للمخاطر ووضع خطط عمل موضع تنفيذ لتحقيق الاســتجابات المناســبة. ويدعو إطار (COSO ERM) إلى مواجهة المخاطر التــي يتعين النظر فيها وتقييمها على مســتوى الكيان أو على مســتوى المحفظة وتقييمها وتقديرها لكل وحدة من وحدات العمل الفردية أو تقســيمها حســب الإدارة أو حســب الوظيفة وأســاليب مماثلة للنظر في مخاطر المؤسســة. وينبغي بعد ذلك تلخيص المخاطر بناء على أثرها وتكرار حدوثها. وكما هو مبين في الشــكل التوضيحي (٨-٧)، يعد هذا أحد أنواع الاتصالات المستخدمة الذي من شأنه أن يساعد الإدارة العليا ومجلس الإدارة في فهم محفظة من المخاطر التي تواجه المؤسسة.

شكل توضيحي (٨-٧)

عرض محفظة ملخص المخاطر



مكونات إطار(COSO ERM): أنشطة الرقابة:

إن الأنشــطة الرقابية لإطار (COSO ERM) هي السياسات والإجراءات اللازمة لضمان تنفيذ الاســتجابات للمخاطر التي تم تحديدها. وعلى الرغم من أن بعض هذه الأنشــطة قد تكون مرتبطة فقط بالاستجابة للمخاطر التي تم تحديدها والمخاطر المقبولة في منطقة واحدة من المؤسســة، فإنها تتداخل غالبــاً من خلال الإدارات والوحدات المتعددة. ويجب أن ترتبط أنشــطة الرقابة الخاصة بإطار (COSO ERM) بشكل وثيق مع عنصر الاستجابة للمخاطر الذي سبق مناقشته.

وبعد أن يتم اختيار الاســتجابات المناسبة للمخاطر، يجب على إدارة المؤسسة اختيار أنشطة الرقابة الضرورية لضمان أن استجابات المخاطر تلك يتم تنفيذها في الوقت المناسب

وبطريقــة فعالة. إن عمليــة مراجعة مدى صحة تنفيذ أنشــطة الرقابة في العادة تكون مشــابهة جداً للعمليات التي تُمارس على أنها جزء من البند ٤٠٤ من قوانين SOx الخاص بتقييــمات الرقابة الداخلية[٧] التــي تم الحديث عنها في الفصل الثــاني من هذا الكتاب. ويمكن تنفيذ أنشــطة الاســتجابة للمخاطر الخاصة بإطــار (COSO ERM) بالخطوات التالية:

١- تحقيق فهم قوي للمخاطر المؤثرة التي تم تحديدها ووضع إجراءات رقابية لمتابعة تلك المخاطر أو تصحيحها.

٢- وضع إجراءات اختبارية لتحديد ما إذا كانت تلك الإجراءات الرقابية المتعلقة بالمخاطر تعمل على نحو فعال أم لا.

٣- أداء اختبــارات لإجــراءات الرقابة لتحديد ما إذا كانــت عملية متابعة المخاطر التي تم اختبارها تعمل بشكل فعال وكما هو متوقع أم لا.

٤- إجراء التعديلات أو التحسينات الضرورية لتحسين عمليات متابعة المخاطر.

هذه العملية ذات الخطوات الأربع هي في الأساس ما تخضع له المؤسسات من متطلبات قانــون SOx التي كانت تقوم بمراجعة عمليات الرقابــة الداخلية لديها واختبارها والتأكيد على أنها تعمل بشكل مناسب. ويوجد فرق رئيسي هنا مضمونه أن المؤسسة مطالبة بشكل قانــوني بالامتثال لإجراءات قانــون SOx من أجل التأكيد على ملاءمــة ضوابطها الداخلية لمدققيهــا الخارجيين. ولا توجد مثل هــذه المتطلبات القانونية مع إطار (COSO ERM). وينبغي أن تســعى المؤسسة لتثبيت أنشطة رقابية لمتابعة المخاطر من أجل تقييم المخاطر المختلفــة التي قامت بتحديدها. وبســبب الطبيعة الحساســة للعديد مــن المخاطر التي تتعرض لها المؤسســة، فإن المتابعة الإدارية للمخاطر تكون حساســة جداً بالنسبة للسلامة العامة للمؤسسة نظراً لطبيعة المخاطر المختلفة التي قد تواجهها.

إن العديد من الأنشــطة الرقابية المندرجة تحت الضوابــط الداخلية الصادرة عن لجنة المنظــمات الراعيــة (COSO) تكون ســهلة التحديــد والاختبار إلى حد ما نظــراً للطبيعة المحاسبية بالنسبة للكثيرين، وهي بشكل عام تشمل ما يلي:

- **فصل المهام:** إن المفهوم الأســاسي للرقابة هو أن الشخص الذي يبدأ المعاملة لا ينبغي أن يكون هو الشخص نفسه الذي يقوم باعتماد تلك المعاملة.
- **مســارات التدقيق:** ينبغي تنظيم العمليات، فمثــل هذه النتائج النهائية يمكن أن تعزى بسهولة إلى المعاملات التي تكون قد تسببت في وجود تلك النتائج.
- **الأمن والسلامة:** يجب أن يكون لعمليات الرقابة إجراءات رقابية مناسبة، وفي مثل هذه الحالة يمكن للأشخاص المخولين فقط مراجعتها أو تعديلها.
- **التوثيق:** يجب أن تكون العمليات موثقة بشكل مناسب.

إن تلك الإجراءات الرقابية، وغيرها، يســهل اســتيعابها بشــكل جيد إلى حد ما، وتقبل التطبيق على جميع عمليات الرقابة الداخلية المعمول بها في المؤسســة، كما أنها تنطبق إلى حد ما على كثير من الأحداث المتعلقة بالمخاطر. فالعديد من كبار المديرين يمكنهم بسهولة تحديد بعض الضوابط الأساسية اللازمة في العديد من عمليات الأعمال. فعلى سبيل المثال، إذا طُلــب منهم تحديد نوعيات معينة من الضوابط الداخليــة التي ينبغي أن تُبنى داخل نظــام تقنية المعلومات الخاص بحســابات المدفوعات، فإن العديد من المهنيين ســيقومون بتحديــد نقاط رقابــة هامة كوجوب اعتماد الشــيكات الصادرة من النظــام من قِبل عدة أشخاص، كما يجب أن تكون السجلات المحاسبية في موضع التنفيذ لتتبع الشيكات الصادرة، كما ينبغي أن تكون عملية إصدار الشــيك للأشــخاص المخولين فقط ممن يمكنهم بدء مثل هذه المعاملات المالية. وتعد هذه بشــكل عام إجراءات الرقابة المفهومة جيداً وعلى نطاق واسع. وتواجه المؤسسة غالباً مهمة أكثر صعوبة في تحديد أنشطة الرقابة لدعم إطار إدارة المخاطر المؤسسية الخاص بها.

وكما تحدثنا سابقاً، فكجزء من مكون تحديد أحداث إدارة المخاطر المؤسسية (ERM)، فــإن الإدارة تحتاج إلى التفكير في فئات المخاطر هذه من حيث مجالات المخاطر الرئيســية لعمليــات التشــغيل، مثل الإيــرادات والشراء وإنفــاق رأس المال، ونظــم المعلومات. كما يمكن تعريف أنشــطة رقابية بعينها تتعلق بالمخاطر داخل كل فئة من هذه الفئات، ســواء للمؤسسة بكاملها أم التي تغطي وحدة أو إدارة ما. وبالرغم من عدم وجود مجموعة من الأنشــطة الرقابية المقبولة أو المعيارية الموحدة لإدارة المخاطر المؤسسية حتى هذا الوقت، فإن وثائق إطار (COSO ERM) تشير إلى عدة مجالات على النحو التالي:

- **مراجعات المستوى الأعلى:** بينما تكون الإدارة العليا غافلة إلى حد ما عن إجراءات الرقابة الداخلية الخاصة بـ"هل الحسابات المدينة تساوي الحسابات الدائنة؟" التي تغطيها فرق ومدققو الحسابات المالية لديها، فإنهم يجب أن يكونوا على علم تام بأحداث المخاطر التي تم تحديدها داخل الوحدات التنظيمية، وينبغي إجراء مراجعات بصورة منتظمة وعلى مستوى عالٍ حول وضع المخاطر التي تم تحديدها وكذلك التقدم المحرز في استجابات المخاطر. هذا النوع من المراجعة المنتظمة إلى جانب الإجراءات التصحيحية المناسبة العالية المستوى يُعد نشاط الرقابة الرئيسي لإدارة المخاطر المؤسسية.
- **الإدارة الفنية أو الوظيفية المباشرة:** بالإضافة إلى المراجعات ذات المستوى الأعلى المذكورة، فإنه ينبغي أن يكون لمديري الوحدات الوظيفية والوحدات المباشرة دور رئيسي في متابعة الأنشطة الرقابية للمخاطر. وهذا أمر مهم ولا سيما في المؤسسات الكبيرة والمتنوعة حيث لا يجب أن تتم الأنشطة الرقابية على مستوى وحدة محلية فحسب، ومن ثم دفع الهرم التنظيمي إلى مستوى إدارة مركزية معينة. وبدلاً من ذلك، يجب أن تتم أنشطة الرقابة ذات الصلة بالمخاطر في إطار وحدات تشغيل منفصلة، في ظل اتصالات وحلول المخاطر التي تقع عبر قنوات المؤسسة.
- **معالجة المعلومات:** سواء كانت عمليات نظم تقنية معلومات أم أشكالاً أكثر بساطة كورقة أو رسائل، فإن إجراءات معالجة المعلومات تمثل عنصراً أساسياً في الأنشطة الرقابية المتعلقة بالمخاطر الخاصة بالمؤسسة. إن إجراءات الرقابة المناسبة هنا، مع التركيز على عمليات تقنية المعلومات للمؤسسة ومخاطرها، تم الحديث عنها بمزيد من التفصيل في الفصل الرابع عشر من هذا الكتاب حول تطبيق النظم المتكاملة.
- **الضوابط المادية:** يوجد العديد من الأحداث المتعلقة بالمخاطر تشتمل على أصول مادية كالمعدات والمخزون والأوراق المالية، ومرافق مادية كمصنع. وسواء كانت هذه الإجراءات المادية تتعلق بالجرد أم بعمليات التفتيش أو أمن أحد المصانع، فإنه يجب على المؤسسة أن تضع إجراءات ملائمة للأنشطة الرقابية المادية القائمة على المخاطر.
- **مؤشرات الأداء:** توظف المؤسسة الحديثة النموذجية اليوم مجموعة واسعة من أدوات إعداد التقارير المالية والتشغيلية. ويمكن استخدام العديد من هذه الأدوات كما هي

أو بعــد التعديل عليها لدعم إعداد تقارير الأداء المرتبطة بأحداث المخاطر. وفي كثير من الحــالات، يمكن تعديل أدوات الأداء الكلي للمؤسســة لدعم هذا المكون المهم للنشــاط الرقابي.

- **الفصــل بــين المهام:** هذا هو النشــاط الرقابي التقليــدي، ســواء كان للضوابط الداخلية لإجراءات العمل أو إدارة المخاطر. فالشخص الذي يبدأ إجراءات معينة لا ينبغي أن يكون هو الشخص نفسه الذي يجيز أو يوافق على تلك الإجراءات. هذا النشاط الرقابي الرئيسي مهم، ســواء كان ذلك في وحدة أعمال صغــيرة يُطلب فيها من مشرف الموظف أن يفحص ويوافــق على إجراءات الموظف أم من خلال الرئيس التنفيذي الذي يجب أن يحصل على الموافقة الرقابية من مجلس الإدارة.

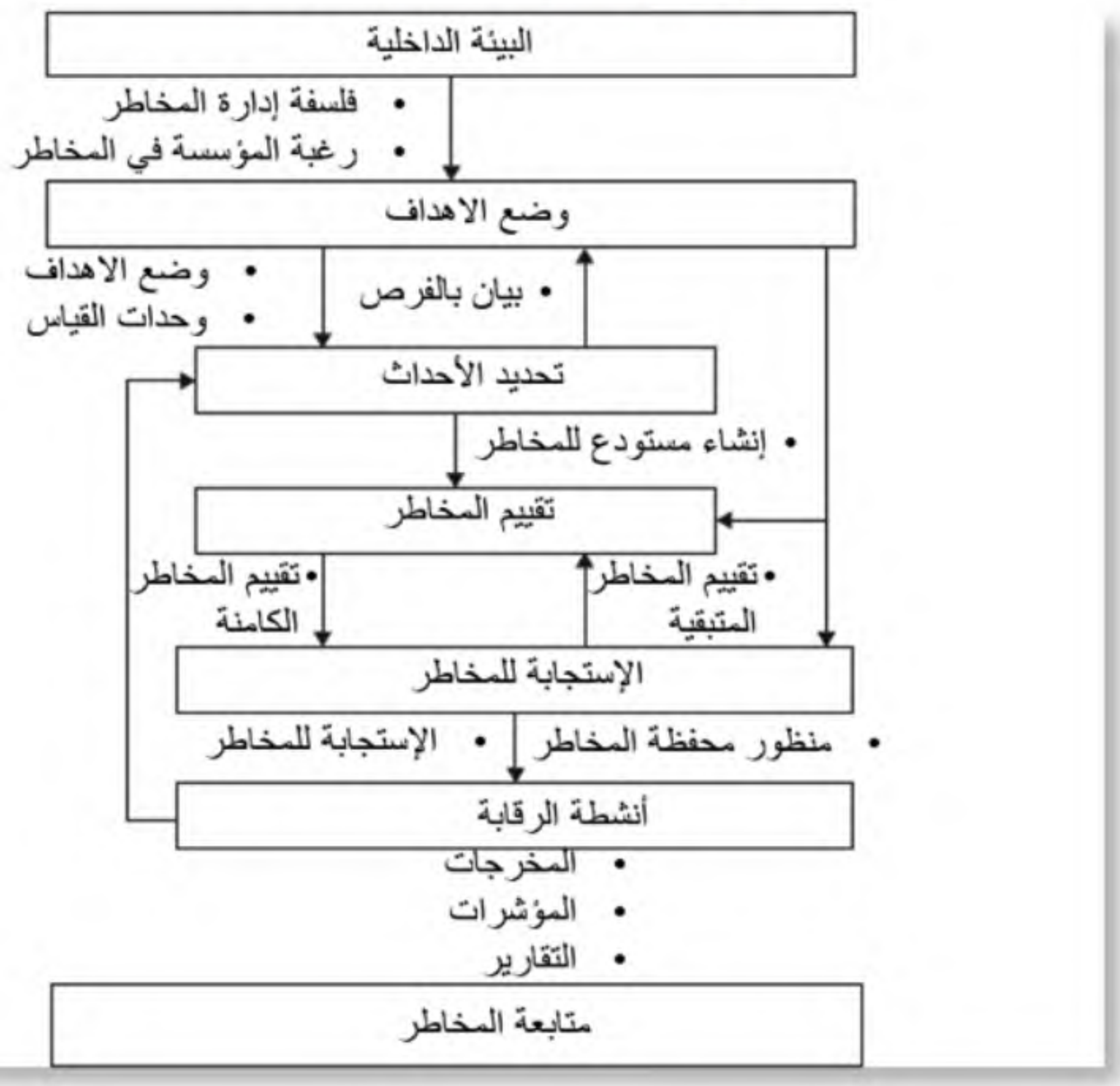
إن هذه الأنشطة الرقابية الخاصة بإطار (COSO ERM) يمكن توسيعها لتشمل مجالات أخرى رئيسية. ويكون بعضها مخصصاً للوحدات المستقلة داخل المؤسسة، إلا أن كل نشاط من هذه الأنشــطة، سواء كان بشكل فردي أم جماعي، ينبغي أن يكون من العناصر المهمة في دعم إطار إدارة المخاطر المؤسسية للمؤسسة.

مكونات إطار (COSO ERM): المعلومات والاتصالات:

عــلى الرغم من وصف المكون الخاص بالمعلومات والاتصــالات على أنه بند منفصل في الشــكل التوضيحــي (٨-١) من إطار (COSO ERM)، فإنه يصــف مجموعة من الأدوات والعمليــات التي تربط بين المكونات الأخرى لإطار (COSO ERM). إن مكون المعلومات والاتصــال هذا يربط جميع المكونات الأخرى بعضها مع بعض. ويبين الشــكل التوضيحي (٨-٨) تدفقات المعلومات والاتصالات عبر مكونات (COSO ERM) الأخرى. فعلى ســبيل المثال، يتلقى مكون استجابة المخاطر مدخلات المخاطر المتبقية والمتأصلة من مكون تقييم المخاطــر وكذلــك دعم درجة تحمــل المخاطر من مكون وضع الأهــداف. ثم يقوم مكون اســتجابة المخاطر الخاص بــإدارة المخاطر المؤسســية (ERM) بتقديم اســتجابة المخاطر وبيانات محفظة المخاطر إلى أنشــطة الرقابة، وكذلك التغذية الراجعة لاستجابة المخاطر إلى مكــون تقييم المخاطر. وبالنظر إلى مكون المتابعــة كونه قائماً بمفردة، نجد أنه لا يوجد به اتصال معلومات مباشر، لكن به مسئولية شاملة عن مراجعة كل هذه الوظائف.

شكل توضيحي (٨-٨)

تدفق المعلومات والاتصال عبر مكونات ERM



وبينما يكون من السـهل نسبياً رسـم مثل هذا المخطط البسيط للتدفق لبيان الكيفية التـي ينبغي أن تُرسـل بها المعلومات من أحد مكونات إطـار (COSO ERM) إلى الآخر؛ فـإن تلك العمليـة تكون في كثير من الأحيان أكثر تعقيداً في ربط مختلف مسـارات النظم والمعلومات معاً. فلدى العديد من المؤسسـات شـبكة ويب معقدة من نظم معلومات لا تقوم دائمـاً على نظم معلومات مرتبطة بشـكل جيد لخدمة عملياتها التشـغيلية والمالية الأساسـية. وتصبح هـذه الروابط أكثر تعقيـداً عند محاولة ربط عمليـات إدارة المخاطر المؤسسـية المختلفة نظراً لأن العديد من التطبيقات الأساسية للمؤسسات لا تتلائم بشكل مباشر مع عمليات تحديد المخاطر وتقييم المخاطر واستجابة المخاطر.

ستكون تلك المبادرة الخاصة بإدارة المخاطر المؤسسية قليلة القيمة ما لم يتم إيصال رسالة حول أهمية هذه المبادرة الخاصة بإدارة المخاطر المؤسسية (ERM) إلى جميع أصحاب المصلحة في المؤسسة. ففي كثير من الأحيان ينبغي أن يكون ذلك في شكل رسالة موجهة من الرئيس التنفيذي (CEO)، والفكرة من وراء ذلك هي إيصال رسالة توضح أهمية إدارة المخاطر المؤسسية في جميع أنحاء المؤسسة. وهذه النوعية من الرسائل تكون ذات قيمة عالية، وخاصة عندما ترغب المؤسسة في إيصال رسالة، على سبيل المثال، مفادها أنه على جميع أصحاب المصلحة أن يكونوا حذرين جداً بشأن تبني بعض المشاريع التي قد تنطوي على مخاطر. وتكون العملية أكثر صعوبة إذا كانت المؤسسة تريد أن تفيد بأنه يجب أن نترك بعض العوامل خارج نطاق سيطرتنا قليلاً ويجب علينا تقبل بعض المخاطر أحياناً. إن الرسالة التي يتم تفسيرها بشكل غير صحيح يمكن أن تفتح الباب على مصراعيه بشكل فعال وبشكل غير ملائم للقرارات والمشاريع المحفوفة بالمخاطر.

مكونات إطار (COSO ERM): المتابعة

تم وضع هذا المكون في قاعدة مجموعة المكونات الأفقية للإطار، فالمتابعة في إطار (COSO ERM) ضرورية لتحديد ما إذا كانت جميع عناصر إدارة المخاطر المؤسسية المثبتة لا تزال تعمل على نحو فعال أم لا. ويقوم أفراد المؤسسة بتغيير عمليات الدعم وتنفيذها وكذلك الشروط الداخلية والخارجية المحيطة. ولبناء مستوى معين من الثقة لدى جميع الأعضاء في المؤسسة في أن إدارة المخاطر المؤسسية لديهم تعمل بشكل فعال ودائم، لابد من وضع عنصر المتابعة الخاص بإدارة المخاطر المؤسسية وتفعيله.

إن عمليات المتابعة الجارية يمكن أن تكون وسيلة فعالة للإشارة إلى الاستثناءات أو الانتهاكات التي تحدث في عملية إدارة المخاطر المؤسسية بشكل عام. ولوضع إطار فعال لإدارة المخاطر، لابد من توسيع نطاق هذه المتابعة لتشمل المراجعات الجارية حالياً لجميع العمليات الخاصة بإدارة المخاطر المؤسسية التي تمتد من عملية تحديد أهداف الأنشطة الرقابية الخاصة بإدارة المخاطر المؤسسية الجارية حالياً إلى أن تصل إلى سير عمل تلك الأنشطة والتقدم الحاصل بها. وقد تشمل المتابعة الخاصة بإطار (COSO ERM) الأنشطة التالية:

- تطبيق آلية إدارية قوية ومستمرة لرفع تقارير عن الأوضاع النقدية ومبيعات الوحدة وغيرها من البيانات المالية والتشغيلية الرئيسية. ولا يجب على المؤسسة المنظمة تنظيماً جيداً أن تنتظر حتى نهاية الشهر المالي أو ما هو أبعد من ذلك لإعداد مثل هذه النوعيات من تقارير الحالة التشغيلية والمالية. وينبغي توسيع نطاق أدوات إعداد التقارير لتشمل مقاييس رئيسية لإدارة المخاطر المؤسسية، متضمناً ذلك بعض أشكال التقارير الخاطفة التي تجري على جميع المستويات المناسبة للمؤسسة.
- يجب وضع عمليات خاصة برفع تقارير دورية لمتابعة الجوانب الرئيسية لمعايير المخاطر المعمول بها، متضمنة أموراً كمعدلات الخطأ المقبولة أو العناصر المرتقبة. فبدلاً من مجرد الإبلاغ عن إحصائيات دورية، ينبغي لمثل هذه التقارير أن تؤكد التنبيهات المتعلقة بالمخاطر مثل الاتجاهات والمقارنات الإحصائية مع الفترات السابقة.
- الإبلاغ عن الوضع الحالي والدوري للنتائج المتعلقة بالمخاطر والتوصيات الواردة في تقارير التدقيق الداخلي والخارجي.
- تحديث المعلومات المتعلقة بالمخاطر باستخدام مصادر كالقوانين الحكومية المنقحة واتجاهات الصناعة والأخبار الاقتصادية العامة. ونؤكد مرة أخرى أنه ينبغي أن يكون هذا النوع من التقارير الاقتصادية والتشغيلية متاحاً للمديرين على جميع المستويات.

وتشير متابعة التقييم المستقل أو الفردي إلى المراجعات التفصيلية لعمليات المخاطر الفردية التي يقوم بها مراجعٌ مؤهلٌ، مثل إدارة التدقيق الداخلي. وقد تقتصر المراجعة هنا على مجالات محددة أو تشمل عملية إدارة المخاطر المؤسسية الكاملة لوحدة تنظيمية. وفي هذا النوع الأخير من المراجعة يمكن الاستعانة بخبراء استشاريين خارجيين مؤهلين لتقييم فاعلية إدارة المخاطر المؤسسية في المؤسسة بأكملها. ومن ناحية أخرى، فبالنسبة للعديد من المؤسسات، قد تكون مؤسسة التدقيق الداخلي القوية هي المصدر الداخلي الأفضل للقيام بتنفيذ مراجعات إدارة المخاطر المؤسسية. وسواء تم ذلك من خلال مدققين داخليين أم مستشارين خارجيين أو كادر من الموظفين المدربين في المؤسسة، فإن أي مراجعة محددة من المراجعات الفردية الخاصة بعمليات إدارة المخاطر المؤسسية قد تستخدم الأدوات التالية:

- **رســم خرائط سير العمليات:** كجزء من أي عملية محددة لإدارة المخاطر المؤسسية، يتعين عــلى الأطراف المســئولة تطوير مخططات توثق عمليات إدارة المخاطر المؤسســية الخاصة بهــم. ويتطلب هذا النظر في الوثائق التي أُعدت لهذه العملية لتحديد ما إذا كانت وثائق العملية صحيحة نظراً للظروف الحالية ولإجراء التعديلات الملائمة على مخططات العمليات.
- **مراجعــات المخاطر والمواد الرقابية:** إن عملية إدارة المخاطر المؤسســية ينتج غالباً عنها كمية كبيرة من المواد الإرشــادية والإجراءات الموثقة وصيغ لتقارير جديدة وما شابه ذلك. وكذلك تكون هناك قيمة حقيقية بالنســبة للفريق المخصــص للقيام بمهام إدارة المخاطر المؤسسية أو لفريق التدقيق الداخلي أو لفريق ضمان الجودة الخاص بالمؤسسة عند قيام أي منهم بمراجعة المواد المتعلقة بالمخاطر والمتابعة من ناحية فاعليتها.
- **المقارنة المعيارية:** ويقصد بها هنا عملية النظر في الإدارات الأخرى المعنية بإدارة المخاطر المؤسســية لتقييم عملياتهم التشــغيلية وتطوير نهج قائم على أفضل ممارسات الآخرين. إن مهمــة جمع هذه المعلومات للمقارنة بها تكون غالباً مهمة صعبة عندما تمتنع في كثير من الأحيان المؤسســات المتنافســة عن تبادل البيانات التنافســية. وتعمل هذه العملية بشــكل مثالي عندما يكون هناك اتصالات وعلاقات مهنية محسنة ومباشرة من نوع واحد لواحد، ومعلومات عن الطريقة التي اســتخدمها البعض لحل بعض المشاكل المماثلة التي تكون غالباً قيمة ومفيدة للغاية.
- **الاستبيانات:** طريقة جيدة لجمع المعلومات من مجموعة واسعة من الناس، ويمكن إرسال الاستبيانات إلى أصحاب المصلحة المعنيين مع طلبات الحصول على معلومات محددة. يعد هذا أســلوب قيــم للمتابعة عندما يكون المســتهدفون من الاســتطلاع منتشرين في أماكن جغرافية مختلفة، مثل مسح متابعة المخاطر للعاملين في مؤسسة تجزئة على الصعيد الوطني.
- **جلســات ميسرة:** يمكن جمع معلومات قيمة غالباً من خلال سؤال أشخاص يتم اختيارهم للمشاركة في جلسة مجموعة التركيز يرأسها قائد مؤتمر ذو مهارة. وهذا هو النهج المتبع من قبل العديد من المؤسســات لجمع معلومات بحوث السوق من خلال ما يسمى بمجموعات التركيز. ويمكن لهذا النهج العام نفســه أن يســتخدم لجمع فريق من الناس - في كثير من الأحيان من المناصب المختلفة في المؤسسة - لمراجعة وضع المخاطر المؤسسية لمجال معين.

إن الغــرض من عملية المتابعة هذه هــو تقييم مدى الجودة التي يعمل بها إطار إدارة المخاطــر المؤسســية في المؤسســة. ولابد من إبــلاغ المديرين المســؤولين في إدارة المخاطر المؤسسية في منطقة محددة يتم حالياً متابعتها وفي المكتب الخاص بإدارة المخاطر المؤسسية بأوجــه القصور الموجودة. إن المفهــوم الكامن وراء متابعة إطــار (COSO ERM) ليس للعثور على أخطاء أو نواقص فحســب، ولكن لتحديد المجالات التي يمكن تحسينها في إطار إدارة المخاطر المؤسسية.

أبعاد أخرى في إطار (COSO ERM):

كما أوضحنا في بداية هذا الفصل وطبقاً لما تم وصفه في الشــكل التوضيحي (٨-١) فإن إطــار (COSO ERM) يكــون عبارة عن إطار ثلاثي الأبعاد بفئاتــه الثمانية باعتبارها بعداً واحداً في الأقســام التي تمت مناقشــتها حالاً. والبعدان الآخــران عبارة عن فئات الأهداف الأربعة له ممثلة بأعمدتها العمودية، وكيانها هو وحداتها الموضحة في البعد الثالث. وعلى الرغم من أن فئات إدارة المخاطر المؤسســية الثمانية التي تم وصفها حالاً مهمة جداً لفهم إطار (COSO ERM) واستخدامه، فإن هذين البعدين الآخرين للإستراتيجيات والوحدات التنظيمية هامان أيضاً. ولفهم المخاطر المحيطة بالأهدأف التنظيمية، يجب على المرء تقييم تلــك المخاطــر من حيث ربما مخاوف الإبــلاغ المرتبطة بهذه المخاطــر والوحدة التنظيمية المعنية التي تصبح التركيز الرئيسي للمخاطر.

إن إطار (COSO ERM) يلزم استيعابه من خلال كل الأبعاد الثلاثة الخاصة بإطار إدارة المخاطر المؤسسية، كما أن العملية الفعالة لإدارة المخاطر، مهما كانت مصممة بشكل جيد ويتم تشغيلها بصورة جيدة، فهي توفر فقط الضمان المعقول - لكنه ليس المرغوب - الذي تحقق به المؤسسة أهدافها المتعلقة بالمخاطر في إطار الفلسفة الإدارية والرغبة في المخاطرة التــي تم وضعهــا. ومع ذلك، فلا يهم إن كانت إدارة المخاطر المؤسســية قد تم تصميمها وإدارتها بشكل جيد، إذ يمكن أن توجد إخفاقات ناتجة عن أخطاء بشرية أو أحداث مخاطر ناجمة عن أي من أحداث كثيرة غير متوقعة.

"الكتاب الأحمر" لنموذج الحوكمة وإدارة المخاطر والامتثال التابع للمجموعة المفتوحة للامتثال والأخلاقيات (OCEG GRC)، وإدارة المخاطر، وحوكمة تقنية المعلومات:

تعــد المجموعة المفتوحــة للامتثال والأخلاقيات (OCEG) منظمــة غير ربحية يقودها قطاع الصناعة، وهي تعمل على تطوير المعايير وتســاعد المؤسســات على تحسين عمليات الحوكمــة وإدارة المخاطــر والامتثال الخاصة بها. وبدعم كبير مــن الصناعة التقنية، قامت مجموعة (OCEG) بوضع نموذج قدرة (GRC) ونشره، ويسمى بـ"الكتاب الأحمر" الصادر عن مجموعة (OECG) مع معايير حوكمة تقنية المعلومات التي أصبحت معترفاً بها بشكل متزايد في العديد من المؤسسات في جميع أنحاء العالم.

ومع التركيز على حوكمة تقنية المعلومات، يســتعرض هذا القســم المواد الإرشــادية لنموذج القدرة (GRC) الصادر عن مجموعة (OCEG) (الكتاب الأحمر). وبينما يكون العديد من هذه المواد الإرشادية مشابهة جداً لغيرها من المعلومات الإرشادية لنموذج (GRC) وإطار إدارة المخاطر المؤسســية الموجودة هنا وفي الفصول الأخرى، فإننا نستشعر بأن مجموعة (OCEG) سوف يكون لها تأثير كبير في حوكمة تقنية المعلومات وعمليات نموذج (GRC) في السنوات المقبلة.

إن اســتخدام مجموعة (OCEG) لكلمة "مفتوحة" في اســمها له معنىً ما يخص تقنية المعلومــات. فالنظام المفتوح يتبــادل بانتظام التغذية الراجعة مــع بيئته الخارجية ليقوم على نحو مســتمر بتحليل تلك التغذية الراجعة، وضبط الأنظمة الداخلية حســب الحاجة لتحقيــق أهداف النظام، ومن ثم ينقل المعلومات الضرورية مرة أخرى إلى تلك البيئة. أما النظــم المغلقة، على عكس النظــم المفتوحة، يكون لديها حدود ثابتة يتم من خلالها تبادل القليل من المعلومات. فالمنظمات التي لديها حدود مغلقة تصبح غالباً راكدة وغير صحية. ومن الأمثلة على الأنظمة المغلقة: البيروقراطية، والاحتكارات، وأنظمة الركود. إن مصطلح "مفتوح" الشــائع الاســتخدام اليوم في العديد من النظم التقنيــة الحديثة والمتطورة يعتبر مصطلحاً مناسباً لنموذج القدرة (GRC).

توجد إرشــادات نمــوذج (GRC) الصادر عــن مجموعــة (OCEG) المفتوحة في وثيقة تسمى الكتاب الأحمر لنموذج القدرة، وتوجد الوثيقة الأساسية على موقع www.oceg.org. ويعود تاريخها إلى شــهر إبريل ٢٠٠٩ في وقت نشرنا، وهي متاحة من خلال شــبكة الإنترنت، في حين توجد نســخة محســنة متاحة للأعضاء المشــتركين. وتتضمن الطبعة الأساسية وصفاً

كاملاً لنموذج (GRC)، لكن النسخة المحسنة ذات التكلفة الإضافية مع القوالب وغيرها من الوســائل المســاعدة تكون أيضاً متاحة. ويرتكز نموذج القدرة هذا حول مفهوم يسمى الأداء القائــم على مبــادئ® Principle Performance، وهو نهج نمــوذج (GRC) المتكامل الذي سوف نناقشه في الأقسام التالية.

كــما يوجد لدى نموذج القــدرة (GRC) الصادر عن مجموعــة (OCEG) العديد من المفاهيم المشابهة تماماً لإطار (COSO ERM) وغيرها من مفاهيم نموذج (GRC) الأخرى التي نوقشت في الفصول الأخرى، وتشمل الأهداف التالية:

- تحسين الأهداف العامة لقطاع الأعمال.
- تحسين ثقافة المنظمة.
- زيادة ثقة أصحاب المصلحة.
- إعداد المؤسسة وحمايتها.
- منع المشاكل والكشف عنها والحد منها.
- الحث على السلوكيات المرغوب فيها وتحفيزها.
- تحسين المسئولية والكفاءة.
- تحسين القيمة الاقتصادية والاجتماعية.

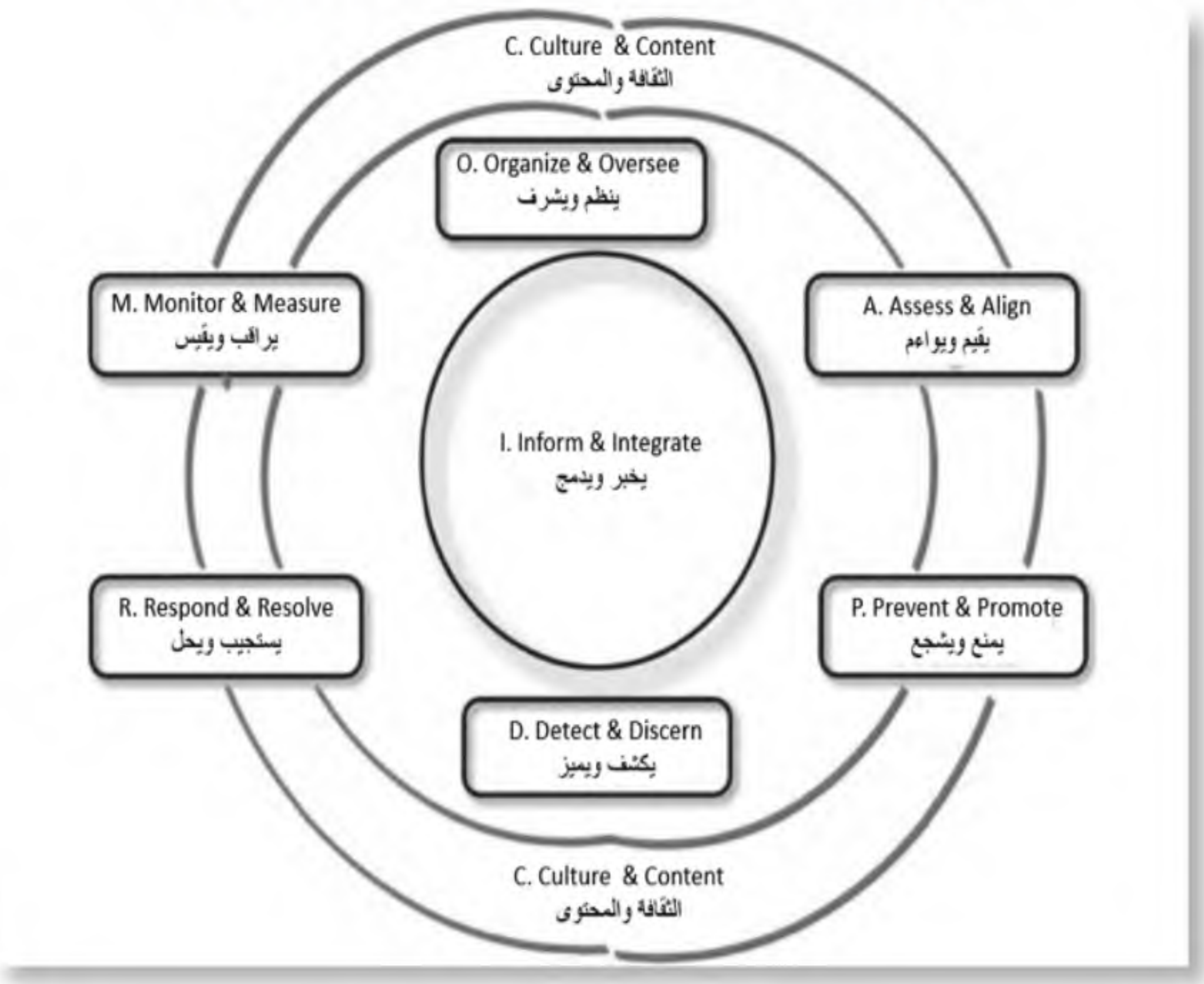
مفهوم الأداء القائم على مبادئ® الخاص بـمجموعة (OCEG) المفتوحة:

حصلــت مجموعة (OCEG) المفتوحة عــلى علامة تجارية لهذا المصطلح وتســتخدم هذا المفهوم لوصف الحاجة إلى صياغة الأهداف المالية وغير المالية للمؤسسة لتحقيق جميع الأهداف التي ترغب المؤسســة فى تحقيقها أثناء اســتخدامها لأســلوب فعال وكفء وقادر على الاستجابة لدعم الحوكمة وإدارة المخاطر والامتثال. إن المفهوم الأساسي هنا هو أن جميع المؤسسات يجب أن تعمــل ضمن حــدود خارجية وداخلية محددة، فالقوى الخارجيــة، مثل المتطلبات القانونية والتنظيميــة، تضع الحدود الخارجية الإلزامية. ويكون الهــدف هو الدمج بين مبادئ وأهداف نموذج (GRC) لمساعدة المؤسسة في أن تعمل على تحسين الأداء بشكل أكثر فاعلية.

ومــن أجل أن تحقق المؤسســة مفهوم الأداء القائم على مبــادئ، يجب عليها أن تحدد بوضوح رســالتها ورؤيتهــا وقيمها وتحديد الأهداف التي تســعى إلى تحقيقها. ويجب أن تحدد كيف ســتحقق هذه الأهداف في الوقت الذي تقوم به أيضاً بمعالجة المخاطر والأمور الضبابية التي تحتمل الشــك وحماية ووضع قيمة مضافــة وتحديد فرص جديدة ومحاولة البقــاء ضمن حدود معينة للســلوك الأخلاقي. ويجب على المؤسســة أن تعمل على جعل هذه الخيارات شــفافة لأصحاب المصلحة الداخليين والخارجيين وأن تحاول تحقيق كل هذا باستخدام نهج متكامل لتحقيق أعلى مستوى ممكن من الأداء.

شكل توضيحي (٨-٩)

نموذج القدرة (GRC) الصادر عن مجموعة (OCEG) المفتوحة



ومن أجل تحقيق الأداء القائم على مبادئ لـمجموعة (OCEG) المفتوحة، يجب على كل كيان أو وحدة في مؤسسة أن تحدد ما هو "الصواب" بالنسبة لها وبعد ذلك تفعل هذه الأشياء الصحيحة بالطريقة الصحيحة. لقد قمنا باقتباس هذا المفهوم من مواد مجموعة (OCEG) المفتوحة، وهو هدف رفيع المستوى يتجاوز المفاهيم التقليدية لتعزيز قيمة أصحاب المصلحة لتشمل النتائج المرجوة التي تلبي مصالح أصحاب المصلحة لدى المؤسسة واهتماماتهم.

وتعـد مفاهيـم الأداء القائم على تلك المبـادئ من العناصر الرئيسـية لنموذج القدرة (GRC) الصـادر عن مجموعة (OCEG) المفتوحة كما هو موضح في الشـكل التوضيحي (٨-٩). وتصف الأقسـام التالية باختصار عناصر هذا النموذج بمزيد من التفصيل، وخاصة عندمـا يكـون لديها أهـداف وغايات مختلفة عـما كانت عليه في الإطـار التقليدي لإطار (COSO ERM) الذي تم وصفه سابقاً في هذا الفصل. ويحدد هذا النموذج مجموعة من المواد والمفاهيم على مسـتوى عالٍ للغاية، وهي تعد جزءاً من نموذج مجموعة (OCEG) المفتوحة. وتشـجيعاً للقـارئ المهتم بهذا الأمر، يمكنه الوصـول إلى نموذج كامل من خلال عنوان الويب الذي أشرنا إليه سابقاً.

إن كل مدخـل من مدخلات النموذج الصادر عـن مجموعة (OCEG) المفتوحة يكون مدعوماً من العناصر الرئيسية أو الفرعية الخاصة بـنموذج (GRC)، فمثلاً حرف C، مشيراً إلى مكون الثقافة والمحتوى يكون مدعوماً في وثائق مجموعة (OCEG) المفتوحة من خلال أربعة عناصر هي:

C1 سياق الأعمال الخارجية (External Business Context)

C2 سياق الأعمال الداخلية (Internal Business Context)

C3 الثقافة (Culture)

C4 القيم والأهداف (Values and Objectives)

وبعد ذلك يتم تقليل رتبة كل عنصر من عناصر نموذج القدرة (GRC) إلى عناصر فرعية لكل منها. فعلى سبيل المثال، بالنسبة للعنصر C3، الذي يشير إلى الثقافة، يحتوي النموذج على العناصر الفرعية التالية:

C3.1 تحليل الثقافة الأخلاقية (Analyze Ethical Culture)

C3.2 تحليل القيادة الأخلاقية (Analyze Ethical Leadership)

C3.3 تحليل ثقافة المخاطر (Analyze Risk Culture)

C3.4 تحليل إشراك مجلس الإدارة (Analyze Board Involvement)

C3.5 تحليل ثقافة الحوكمة وأسلوب الإدارة (Analyze Governance Culture and Management Style)

C3.6 تحليل مشاركة القوى العاملة (Analyze Workforce Engagement)

وكل عنـصر من تلك العنـاصر يكون مدعوماً أيضاً بعنـاصر تفصيلية أكثر لزيادة حجم القائمـة. وبالإضافة إلى ذلك، فإن النموذج يحتوي على مجموعة من المبادئ وقائمة بمصادر الفشل الشائعة لكل مبدأ من هذه المبادئ، فضلاً عن توجيهات ومراجع لمواد دعم إضافية.

ويمكـن إيجاد أهـداف تفصيلية مماثلة لكل مـن العناصر والعناصر الفرعية للشـكل التوضيحـي (٨-١٠). وبالإضافة إلى ذلك، فإن هذا النموذج يحتوي على توثيق الممارسـات الفرعية لكل عنصر من العناصر الفرعية. فمثلاً، عنصر (O)، وهو عنصر التنظيم والإشراف، موجود في المركز العلوي يحتوي على عنصر يسـمى O2، ويشـير إلى الأدوار والمسـئوليات، مع عنصر فرعي O2.4، ويشـير إلى تحديد القواعد التشـغيلية لنظام (GRC) وتمكينها من العمـل. وتوجد توصيفات العناصر والعناصر الفرعية تلك في جميع أنحاء النموذج. فعلى سبيل المثال، يبين الشكل التوضيحي (٨-١٠) أنشطة O2.4.01.

شكل توضيحي (٨-١٠)

مثال على الممارسات الفرعية لنموذج GRC: O2.4 تحديد وتمكين القواعد التشغيلية لنظام GRC.

O2.4.01 تحديد الأدوار والمسئوليات لأنشطة نموذج (GRC) الأساسية التالية:

- المنهجية والسياسة والإجراءات والمعايير والمفردات والصيانة
- تحديد المخاطر والمتطلبات والتحليل والتحسين

- تنفيذ المبادرة / إدارة محفظة المشروعات
- علاقات أصحاب المصلحة
- خط المساعدة أو الخط الساخن
- الاستقصاء والحلول
- قياس الأداء
- الاتصالات متضمنةً العلاقات العامة
- إدارة المعلومات
- التقنية

إن هدفنا هنا ليس وصف كل عنصر وعنصر فرعي من هذه العناصر والأنشطة الخاصة بـمجموعـة (OCEG) المفتوحة بالتفصيل، لكن هدفنا هو وصـف المفاهيم العامة وراء نمـوذج مجموعة (OCEG) المفتوحة. ويمكن للقارئ أن يصل إلى نموذج شـامل من خلال موقع ويب www.oceg.org.

بهـذا الملخص أو التوضيح للنقاط الفرعية والنقـاط المتفرعة منها، يوجد لدينا تفاصيل كافية هنا لمسـاعدة المؤسسة على إنشـاء وتنظيم إدارة للحوكمة وإدارة المخاطر والامتثال (GRC). كما توجد مجموعات جيدة من المبادئ والمصادر المشتركة للإرشادات للمساعدة في تكوين عملية فعالة خاصة بنموذج (GRC) داخل المؤسسـة. وقد لخص هذا القسـم والأقسام السـابقة عناصر نموذج القدرة (OCEG GRC) على مستوى عالٍ للغاية، بعضها مشـابه تماماً لعمليات نمـاذج (GRC) و(COSO ERM) التي تمت مناقشـتها في فصول أخرى. في حين يدعو البعض الآخر لاتباع نهج أكثر تفصيلاً وفي بعض الأحيان إلى نهج موجه بدرجة أكبر نحو نظم رقابة إدارية. لكننا مع ذلك نحتفظ بوصف عالي المسـتوى لا ينصف الدراسة الكاملة التي يمكن العثور عليها في منشور مكون من ٢٤٠ صفحة في شكله الأساسي وبقـدر أكبر من التفصيل في وثيقة مطولة. مما يشـجع القارئ المهتم إلى القيام بمزيد من البحث في نموذج (OCEG GRC).

مستوى هيئة وضع معايير مجموعة (OCEG) المفتوحة ونطاقها:

ليـــس لدى مجموعة (OCEG) المفتوحة في الوقت الحاضر هيئة لوضع المعايير الخاصة بحوكمة تقنية المعلومات كما هو موجود مع هيئات (PCAOB) أو (ISO). وبالإضافة إلى ذلك، وعلى الرغم من أنها أصدرت بعض المواد الإرشادية القوية، فإن تلك المعلومات ما تزال مفتقرة إلى مستوى اعتراف كالموجود من خلال المعايير المهنية مثل تلك الصادرة عن معهد المدققين الداخليين (IIA) أو (ISACA). ومع ذلك، فإننا نرى أن أهمية مجموعة (OCEG) المفتوحة وموادها الإرشادية سيزداد في السنوات القادمة وسوف تنمو الاهتمامات والحاجة لعمليات فعالة لنموذج (GRC).

وتكمن إحدى نقاط القوة الرئيســية لمجموعة (OCEG) المفتوحة في أنها منظمة تطوعيــة تماماً يقوم على إدارتها موظفون جاؤوا على ســبيل الإعارة من المنظمات الراعية، وقــد شــكلوا مجلس قيــادة لمجموعة (OCEG) المفتوحة. يشــمل الرعــاة هنا الشركات المحاســبية العامة الكبرى مثل برايس ووترهاوس كوبرز (PwC) وجرانت ثورنتون (Grant Thornton)، بالإضافة إلى أن هناك العديد من الرعاة من الجهات الرائدة في صناعة تقنية المعلومات الكبرى مثل أوراكل (Oracle) وساب (SAP)، ويأتي في المقام الأول رعاة الصناعة في الولايــات المتحــدة مثل شركة التأمــين الكبرى عون (Aon) ومتاجــر التجزئة وول مارت (Walmart). وإذا كان ثمــة قلــق هنا، فإنه قد يعزى إلى أن مجموعة (OCEG) المفتوحة هي منظمة أمريكية من الأســاس وليســت منظمة دولية في الحقيقــة، لأنها معتمدة على أعضــاء المنظمات وأعضاء اللجــان الراعية لها. وفي عالمنا المعاصر، إننا بحاجة إلى المزيد من الاهتمام الدولي.

وقد يرغب أحد كبار المديرين المهتمين في استخدام مواد مجموعة (OCEG) المفتوحة هذه على أنها أحد المصادر المرجعية الإضافية، إذ إنها مجموعة واسعة من المواد التي يمكننا فقط توقع زيادة أهميتها في السنوات المقبلة.

ملاحظات:

١. Tsunami Pacts and Information," Australian Government, Bureau of" .Meterology. www.bom.gov.au/tsunami/info/index.shtml

٢. Robert R. Moeller, COSO Enterprise Risk Management: Establishing Effective Governance. Risk, and Compliance Processes. 2nd ed. .((Hoboken. NJ: John Wiley & Sons. 2011

٣. Christine Hauser, "Boeing Board Ousts Chief. Citing Relationship with .Executive," New York Times, December 7. 2005

٤. Enterprise Risk Management-Integrated Framework: Application .(Techniques (COSO, April 2004

٥. Scott Patterson. "Breakdown: A Glimpse Inside the 'Plash Crash,'" Wall Street Journal. June 10. 2012. wsj.com/article/SBlOO .0l42405270230329660457745433006603 9896.html?mg=reno64-wsj

٦. اثنين من الباعة اللذين يقومان بتوريد لوحات المعلومات هما موردي البرمجيات بيزنس أوبجيكتس Business Objects وكوجنوس COGNOS.

٧. لمزيـد مـن المعلومـات حول مراجعـات الرقابة الداخليـة الواردة بالبنـد ٤٠٤. انظر Robert Moeller. Sarbanes-Oxley Internal Controls: Effective Auditing " ".(with ASS. CobiT, and ITIL (Hoboken. NJ: John Wiley & Sons, 2008

الجزء الثالث

أدوات وتقنيات إدارة البنية التحتية لحوكمة تقنية المعلومات

الفصل التاسع
حوسبة سحابية وافتراضية وحوسبة محمولة متنقلة

عالم نظم تقنية المعلومات مليء دائماً بالمفاهيم والتقنيات الجديدة المتطورة باستمرار. فبعضها يعد من المفاهيم والتحولات الخاصة بتقنية المعلومات والتي سرعان ما أصبحت ممارسات شائعة ومقبولة. ويمكن اعتبار لغة برمجة الإنترنت الجافا أحد الأمثلة على تلك التقنية الحديثة. فقد أصبحت التطبيقات التي تستخدم الجافا بمثابة الوسيلة التي تسمح بالاتصال بين مواقع الإنترنت المركزية والأنظمة الفردية، كما أصبحت الجافا معياراً لتطوير الإنترنت (شبكة المعلومات العالمية). من ناحية أخرى، فإنه فضلاً عن أن هناك العديد من التقنيات الحديثة التي لاقت في بداياتها المزيد من الاستحسان والدعم والدعاية والترويج في العديد من المطبوعات المتنوعة الخاصة بتقنية المعلومات؛ فإنها لم تحتل مكانة عالية في السوق وسرعان ما تم نسيانها. وفي النهاية، فإن هذه التقنيات "لم تكن تلك الصفقة الكبيرة"، وذلك عندما تم تجاهلها وإهمالها من قبل مستخدمي تقنية المعلومات والسوق التقني أو أن المنافسين قد جاؤوا بعروض أفضل.

لقد كان لدينا بعض التقنيات الحديثة منذ مدة طويلة، وفي الواقع تعد هذه التقنيات حديثة فقط عندما تُقارن بالنظم والعمليات التقليدية لتقنية المعلومات. وقد أسهمت هذه التقنيات في تغيير الطريقة التي نفكر بها في بناء وإدارة نظم تقنية المعلومات والعمليات الداعمة لها. وسوف يقوم هذا الفصل بتسليط الضوء على ثلاث من هذه التقنيات الحديثة التي أصبحت شائعة بشكل متزايد في عمليات تشغيل تقنية المعلومات في الوقت الراهن، فيما ستطرح أيضاً كل تقنية من هذه التقنيات بعض القضايا الخاصة بحوكمة تقنية المعلومات.

في البداية سنتحدث عما أصبح يعرف بالحوسبة السحابية Cloud Computing، وهو المفهوم المرتبط باستخدامنا للإنترنت وشبكة الويب العالمية منذ أواخر التسعينيات من القرن الماضي. يستخدم المهنيون هذه الأيام إحدى أدوات البحث عبر الإنترنت كجوجل مثلاً للبحث عن إجابات لأسئلة أو لجمع المزيد من المعلومات عن موضوع ما. وبينما ينتج

وبشكل فوري عن أحد طلبات البحث التقليدية مدى واسع من "ضربات" أو نتائج البحث لهذا الطلب، فإننا في الواقع لا نفكر كثيراً بالطريقة التي من خلالها اســتطعنا الحصول على كل تلك النتائج الهائلة وبتلك السرعة الهائلة. فجميع هذه النتائج تأتي من شبكة الإنترنت، ســواء كانت من بلادنا أو من العالم الخارجي. ونظراً لأننا لا نســتطيع الإشــارة إلى نظام أو مصدر محدد على أنه هو المزود للمعلومات الخاصة باســتعلامنا عبر شــبكة الإنترنت، فإننا نتصــور أن تلك المصادر الخاصة بالإنترنت كما لو كانت عبارة عن شــبكة اتصالات مترابطة وواسعة، تكون غالباً "سحابة" من المصادر.

تتجاوز مصادر تقنية المعلومات، مجرد كونها محركات للبحث، والتي يتم عرضها بشكل متزايد من خلال ســحابة الإنترنت تلك. وسواء كانت تلك السحابة عبارة عن مرفق خدمي محلي أو عالمي أو حتى كانت عبارة عن مركز لإحدى المؤسســات الكبيرة، فنحن نســتخدم الحوسبة السحابية بشكل متزايد لبناء وإدارة نظم تقنية المعلومات الخاصة بنا. وسيناقش هذا الفصل بعض القضايا الخاصة بحوكمة تقنية المعلومات والتي تُثار عندما نستخدم تلك السحابة لنظم وعمليات تقنية المعلومات.

ســتكون الافتراضية virtualization وقضايا حوكمة تقنية المعلومات الخاصة بها هي التقنية الثانية التي سيتم مناقشتها في هذا الفصل. فعلى الرغم من أن لها أصولاً تعود إلى النماذج السابقة الخاصة بنظم الحاسبات المركزية التي تم إنتاجها من قِبَل شركة آي بي إم IBM منذ ســنوات عديدة، فإن الافتراضية هي المفهوم الذي كان مجهولاً بالنسبة لمعظم المهنيين العاملين في مجال تقنية المعلومات حتى فترة زمنية ليســت بالبعيدة. فهي تعود للوقت الذي انتقلنا فيه للمرة الأولى من نظام تقنية معلومات يعتمد على حاسب مركزي واحــد إلى العديد من نظم الخادم المتصلة في تقنية المعلومــات والتي احتوت في البداية عــلى عدد قليل من هذه النظم ثــم زادت بعد ذلك. في البداية كانت عملية توصيل كل نظام خادم بمجموعة من وحدات التخزين والمرفقات الأخرى تعتبر من العمليات السهلة، إلا أن النظــم أصبحت أكثر تعقيداً مع نمو إعدادات نظم تقنية المعلومات. هذا بالإضافة إلى أن إدارة عمليات التشــغيل الخاصة بتقنيــة المعلومات قد أدركت مبكراً أن إعداداتها الخاصة بالموارد المتصلة والملحقة بالخادم لم تكن متوازنة بشكل جيد. فعلى سبيل المثال، قــد يكون للخادم (أ) إمكانيات كبــيرة للذاكرة المؤقتة أو وحدات التخزين الملحقة ولكنه

ربما لا يستخدم كل هذه الموارد على أنها جزء من عمليات التشغيل المجدولة أو الاعتيادية التي تتم على هذا الخادم (أ). في حين قد يكون هناك خادم آخر (ب) به قصور في الموارد ويحتاج إلى بعض الموارد الزائدة عن حاجة الخادم (أ) لتساعده خلال فترة أحمال الحوسبة المرتفعة.

خلال الأيام الأولى للحوسـبة الخاصة بنظم "عميـل - خادم"، كان يتم ربط تلك الموارد بـكل خادم على حدة إما من خلال تعليـمات برمجية محددة أو حتى من خلال توصيلات كوابل مادية. ومن ثم فإن عمل تغييرات كنقل بعض الموارد غير المستخدمة من الخادم (أ) إلى الخادم (ب) ليساعده في إنجاز مهامه كانت تستهلك وقتاً طويلاً وفي بعض الأحيان كانت مهمة معقدة. وقد تم حل تلك المشـكلة الخاصة باتصال الخوادم بموارد تقنية المعلومات وتحقيـق ما يعرف بتوازن الأحمال بين الخوادم عن طريق بعض بائعي نظم إدارة التخزين ابتداءً من العام ٢٠٠٠ تقريباً بواسطة ما يعرف الآن بالنظم الافتراضية.

ففـي البيئة الافتراضية، لا تتصل موارد النظام ببعضها البعض بشـكل حقيقي أو مادي ولكنها ترتبط بشـكل منطقي بواسطة أدوات برمجية خاصة. وبناءً على الطلب على موارد النظم، فإنه يمكن للنظم المنفصلة أن تتصل بشـكل افتراضي مع موارد أخرى، بشـكل آلي أو تلقائي، بدلاً من اسـتخدام الكوابل المادية اليدوية أو الروابط البرمجية التي كانت تستخدم في السابق. حيث تستطيع البيئة الافتراضية تقديم قدرات كبيرة للإعدادات الضخمة لتقنية المعلومـات. من ناحية أخرى، إذا كانت عمليات النظم الافتراضية غير مفهمومة أو مطبقة أو مدارة بالشـكل المناسب، فإنها قد تثير بعض القضايا المتعلقة بحوكمة تقنية المعلومات. سـيقدم هذا الفصل المفاهيم الخاصة بالبيئة الافتراضية لتقنية المعلومات كما يناقش بعض القضايا الرئيسية للحوكمة ذات الصلة بهذا الموضوع.

وسـيختتم هذا الفصل بالحديث عن قضايا حوكمة تقنيـة المعلومات المتعلقة بأجهزة الحوسـبة المحمولة الشخصية الواسعة الانتشار والتي لا تستخدم فقط للاغراض الشخصية وإنما تسـتخدم أيضاً عـلى أنها مكونات لنظـم تقنية المعلومات المؤسسـية. تعتبر أجهزة الحواسـيب اللوحية الصغـيرة أو الهواتف الذكية بمثابـة أدوات رائعة للاتصالات والوصول إلى الإنترنـت والتقـاط الصور الفوتوغرافيـة والعديد من المهام الأخـرى. فعلى الرغم من

إطلاقها على أنها أجهزة شخصية، فإنها تسببت في نجاحات كبرى في أماكن العمل. وسَيُخْتَم هذا الفصل بمناقشة قضايا حوكمة تقنية المعلومات المتعلقة باستخدام أجهزة الحاسبات الشخصية في بيئة العمل.

التعرف على الحوسبة السحابية:

كان لدى مديري الأعمال القدامى، الذين نشؤوا في عصر الورق والقلم الرصاص، ولسنوات، اعتقاد بأن بعض أعضاء فرق نظم وتطوير تقنية المعلومات العاملين لديهم لهم "مديرون في السُحُب"، في حين أن ما يعرف بالحوسبة السحابية يعد من المفاهيم الحديثة والمتطورة والمهمة بالنسبة للعديد من عمليات تشغيل تقنية المعلومات. وهو وثيق الصلة بالمفاهيم الخاصة بالبنية الموجهة نحو الخدمات SOA (Service-Oriented Architecture) والتي نوقشت في الفصل الثالث عشر من هذا الكتاب، لقد أسهمت الحوسبة السحابية في تغيير الأسلوب المتبع من قبل العديد من المؤسسات في بناء واستخدام تطبيقات تقنية المعلومات.

يُستخدم مصطلح السحابة غالباً هنا وفي العديد من المراجع المنشورة على أنه تعبير مجازي للدلالة على الإنترنت. إن الفكرة التي تكمن خلف سحابة الإنترنت تلك هي أن المستخدمين ليسوا بحاجة إلى (معرفة بـ أو خبرة عن، أو سيطرة على) البنية التحتية للتقنية "في السُحُب" التي تدعم التطبيقات القائمة على الإنترنت. وقد تم استحداث هذا المصطلح في مجال صناعة الهواتف، حيث ظل قائماً حتى تسعينيات القرن الماضي، فالبيانات وحتى الدوائر البدائية لشبكة الإنترنت بين الأماكن قد تم ربطها من خلال الأسلاك. ثم بدأت بعد ذلك شركات الهواتف البعيدة المدى بتقديم خدمات الشبكة المحلية الافتراضية اللاسلكية لنقل البيانات. وقد أسهم نمو تلك الشبكات اللاسلكية والإنترنت وشبكة الويب العالمية في تطوير الطريقة التي نفكر فيها بخدمات تقنية المعلومات هذه الأيام.

إن الحوسبة السحابية، على كل حال، تعد أكثر من مجرد شبكة إنترنت، فهي الطريقة التي نستخدمها نحن للتفكير بالخدمات التي تقدمها التطبيقات التي تسكن شبكة الإنترنت. ولأنه من المستحيل أن يكون هناك تحديد مسبق لمسارات حركة الإنترنت بشكل دقيق، فقد تم استخدام مصطلح السحابة ليدل مجازاً على المرافق الخاصة بخدمات تقنية المعلومات والتي تعد أحد مسئوليات مقدمي الخدمات، إضافة إلى البنية التحتية للشبكة.

وسرعان ما تبع ذلك كل من مفاهيم المنتجات البرمجية أو الخدمات عبر الإنترنت أو مفهوم البنية الموجهة نحو الخدمات SOA.

يقوم بائعو البرمجيات عادة بعرض المنتجات البرمجية الخاصة بهم على شكل خدمات على الإنترنت بدلاً من أن تكون على شكل تطبيقات تسكن خوادم العملاء الشخصية. وخير مثال هنا - أحد رواد مثل هذا النوع من المنتجات - هو مورد البرمجيات الخاصة بإدارة علاقات العملاء سيلزفورس (www.salesforce.com/crm/products.jsp) (SalesForce). فهذا المورد للأدوات البرمجية الخاصة بتتبع العملاء والمبيعات لا يقوم ببيع منتجاته كمجموعة من البرامج المحملة على الأقراص المدمجة CDs ليقوم العميل باستخدامها. لكنه يقوم بعرض جميع البرامج والوثائق الخاصة بشركة SalesForce على شبكة الإنترنت، حيث يقوم العملاء بدفع المال مقابل المنتجات البرمجية فقط عندما يستخدمونها. حيث تُستخدم تطبيقات شركة SalesForce على شكل خدمات مقدمة للعملاء.

يوضح الشكل التوضيحي (٩-١) هذا المفهوم الخاص بالحوسبة السحابية. وقد قمنا بتسليط الضوء على مقدمي الخدمات الذين يقومون بعرض منتجات خاصة بالحوسبة السحابية هذه الأيام مثل شركة أمازون Amazon وشركة جوجل Google وشركة مايكروسوفت Microsoft وشركة سيلز فورس Salesforce كذلك. وما هذه إلا عينة بسيطة عن بعض التطبيقات الحالية، وبالتأكيد هناك ما هو أكثر بكثير. وفيما يلي بعض فوائد التطبيقات التي تعمل في بيئة الحوسبة السحابية:

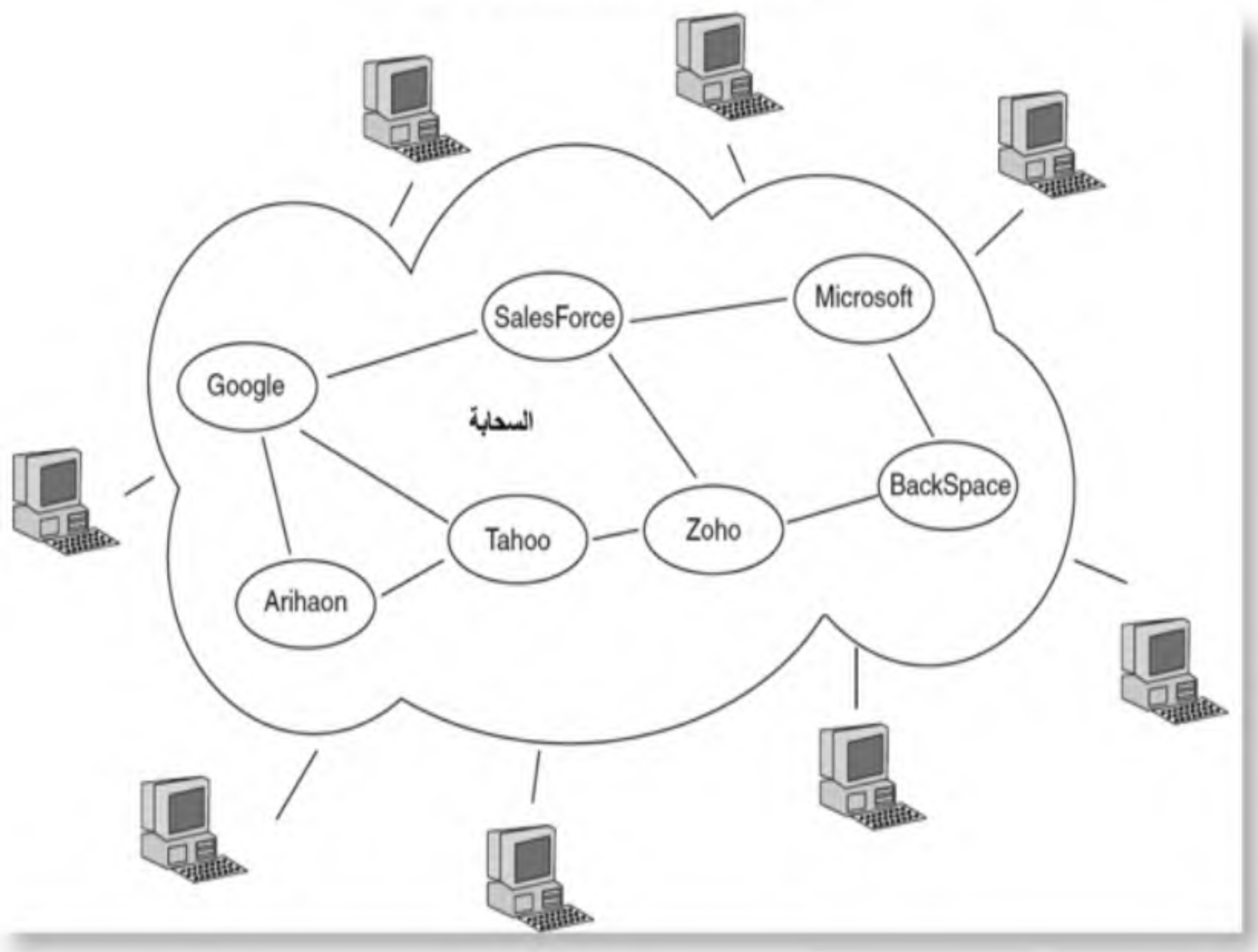
- **خفض تكاليف البنية التحتية نتيجة المركزية:** مع وجود تطبيقات تقنية المعلومات على البيئة السحابية، لم يعد هناك حاجة للحفاظ على المستوى نفسه من العمليات الخاصة بإدارة التغييرات البرمجية وغيرها من الضوابط المتعلقة بتلك التطبيقات الموجودة في البيئة السحابية. قد يكون لهذا الأمر إلى حد ما جانب إيجابي وآخر سلبي بالنسبة للبعض نظراً لأنك تحصل فقط على السمات والأشكال التي يسمح بها التطبيق.
- **ارتفاع سقف سعات الأحمال:** يمتلك مقدمو الخدمات السحابية كشركة أمازون أو جوجل مزارع خوادم ضخمة جداً لنظم تقنية المعلومات وبقدرات تخزينية هائلة، حيث تبدو سعات الأحمال التشغيلية لحواسيبهم وكأنها تقريباً لا محدودة.

- **متابعة الأداء المناسب للنظم من قبل مقدم الخدمة:** يستطيع مقدمو الخدمات السحابية أن يقوموا بمراقبة جميع خدمات تقنية المعلومات المقدمة من مزود البيئة السحابية وكذلك مراقبة المستخدمين المهمين. ونتيجة لذلك يجب أن يكون لدى مقدم الخدمة أدوات رقابية معمول بها لتقديم تغييرات التحسين الخاصة بالعملية بالشكل المطلوب.

- **مرونة التطبيقات وخدمات تقنية المعلومات:** لقد قام مقدمي خدمات البيئة السحابية بعمل نسخ طبق الأصل للحلول -وهو ما يعرف باسم (المرآوية) mirroring - التي يمكن أن تستخدم في حالات الكوارث أو في توازن الأحمال عند ازدحام البيانات. فسواء كانت هناك كارثة طبيعية تستلزم الحاجة لموقع آخر في منطقة جغرافية مختلفة، أو كان هناك ازدحام شديد للبيانات، إذ يكون مقدمو خدمات البيئة السحابية عادة على استعداد لتقديم الحلول المناسبة.

شكل توضيحي (٩-١)

مفاهيم الحوسبة السحابية



إن مديــري الشركات الذين يقومون بتطبيق حوكمة تقنية المعلومات بحاجة إلى اتباع نهج مختلف في مراجعة الضوابط الداخلية المتعلقة بتطبيقات البنية الموجهة نحو الخدمات SOA بالإضافة إلى فهم الأمور الخاصة بأمن تقنية المعلومات في بيئة الحوســبة الســحابية. لقد أصبحت خدمات شبكة الويب وغيرها من خدمات البنية التحتية تُقَدَّم وبشكل متزايد في البيئة الســحابية، الأمر الذي يستدعي إعادة التفكير ببعض الاعتبارات الخاصة بعمليات التدقيق والرقابة.

مراجعة الضوابط الخاصة بتطبيقات الحوسبة السحابية:

كون التطبيق يعمل انطلاقاً من بيئة البنية الموجهة نحو الخدمات SOA – فهذا لا يعني أبــداً أن الحاجة إلى تقييم وفهــم الضوابط الداخلية الخاصة بهذا التطبيق لم تعد موجودة. بل يجب أن يستمر التطبيق القائم على البنية الموجهة نحو الخدمات في مسارات التدقيق وإجراءات فحص الأخطاء نفســها وغيرها من الممارســات الجيــدة التي يمكن أن نجدها في أي تطبيــق تقنية معلومات محكم الرقابة. في الغالب يمكننا توقع أن تطبيق الأعمال الذي يعمل تحت رعاية إحدى الشركات الكبرى التي تقدم الخدمات السحابية مثل جوجل، الذي يُســتخدم غالباً من قِبل عدد كبير من العملاء في جميــع أنحاء العالم، لديه ضوابط داخلية ملائمة.

تمثل الحوســبة الســحابية تغييراً جوهرياً في الطريقة التي تعمل وتدار بها التطبيقات، وبينما لا يوجد ســوى عــدد محدود من الباعــة الذين يقومون اليــوم بتقديم التطبيقات البرمجية القائمة على الخدمات، فإن هذا الرقم من مقدمي الخدمة مرشــح للزيادة. هناك مســتوى ضمني مــن الثقة في تلك الخدمات المقدمة من قِبــل العديد من مزودي الخدمة تحت مظلة سحب الإنترنت تلك، إلا أن قادة إدارة الأعمال وتقنية المعلومات لتلك الخدمات إلى جانــب مدققي تقنية المعلومات يجب أن يحصلوا عــلى ضمانات بأن هذه التطبيقات القائمة على السحابة تتم مراقبتها بشكل جيد. كما يجب على جميع المستخدمين المباشرين وغير المباشرين للحوســبة الســحابية تطوير مســتوى قوي من الثقة في الخدمات البرمجية والبنية التحتية التي تشكل السحابة الخاصة بالمؤسسة. يجب أن يلتقي المسئول التنفيذي، الذي يحدد ما إذا كان قســم تقنية المعلومات لديه ســيقوم بتبنى إســتراتيجية الحوســبة

السحابية فيما يخص بعض تطبيقاته في المؤسسة، مع إدارة تقنية المعلومات لفهم مثل هذه المبادرات. وفيما يلي بعض القضايا الأساسـية فيما يخص حوكمة وضمان تقنية المعلومات في الحوسبة السحابية:

- **الشـفافية Transparency:** يجب على مقدمي الخدمات السـحابية أن يكونوا قادرين عـلى إثبات وجود ضوابط أمنية فعالة وقوية، تضمن للعملاء بأن معلوماتهم مؤمنة على نحو جيد ضد أي عملية وصول غير مصرح بها ، أو تغيير، أو تخريب. فالأسـئلة الرئيسـية التي توجه لأي مقدم خدمات يعرض التطبيقات السحابية هي:

- ما نوعية الموظفين العاملين لدى مقدمي خدمات البيئة السـحابية الذين يستطيعون الوصول لمعلومات أي عميل؟

- هل يتم الحفاظ على الفصل بين مهام موظفي مقدمي الخدمات السحابية؟

- كيف يتم الفصل بين الملفات والبيانات الخاصة بالمعلومات المختلفة للعملاء؟

- ما الضوابط الموضوعة لمنع أي خروقات أمنية ورقابية في السحابة والكشف عنها والرد عليها؟

- **الخصوصية Privacy:** يجب على مقدمي خدمات الحوسـبة السـحابية إعطاء ضمانات بأن ضوابط الخصوصية المستخدمة ستمنع الخروقات الأمنية وتكشف عنها وترد عليها في الوقت المناسب، وبأن لديها خطوط اتصالات قوية ويتم فحصها بشكل دوري.

- **الامتثـال Compliance:** لكي يتم الامتثال لمختلف القوانـين واللوائح والمعايير المعمول بها، فقد تكون هناك مخاوف متعلقة بالحوسـبة السـحابية من حيث أن البيانات قد لا تُحفظ في مكان واحد بل ربما لا يكون من السـهل اسـترجاعها. فمن المهم جداً ضمان أنه عند طلب البيانات من قبل أصحابها، فإنه يمكن تقديمها دون المسـاس بالبيانات الأخرى. عند اسـتخدام الخدمات السحابية، يجب أن تكون هناك ضمانات بأن المؤسسة تستطيع الحصـول على بياناتها عندما تحتاجهـا، أو أن الجهة المقدمة للخدمة قد تطالب بحقها في حجب البيانات عن السلطات.

- **تدفـق البيانات عـبر الحدود:** مع وجـود احتمالية تخزين المعلومات السـحابية في أي مكان داخل السحابة، فقد يكون معرفة الموقع الجغرافي للمعلومات من إحدى القضايا أو

المشــاكل. فالموقع الجغرافي للبيانات هو الذي يفرض الالتزام القانوني والقضائي للفصل في الدعاوى. ولا يزال هناك العديد من المسائل القانونية التي لم تحل بعد في هذا المجال.

- **الاعتماد:** يجب أن يزود مقدمو خدمات الحوسبة السحابية عملاءهم بالضمانات الكافية على أنهم يقومون بعمل الأشــياء "الصحيحة". لذلك، يجب أن نرى في المســتقبل عمليات تدقيق مستلقة يقوم بها طرف ثالث و/أو تقارير عن الخدمة لأحد المدققين والتي ستصبح جزءاً حيوياً لأي برنامج ضمان يخص مقدم خدمات الحوســبة الســحابية. وســتتبع هذه التقاريــر المعيار الصــادر عن المعهد الأمريكي للمحاســبين القانونيين AICPA والمعروف باسم معيار التدقيق رقم ٧٠ [١] (SAS 70) الذي سيصبح أكثر أهمية في السنوات القادمة.

إن وجود المعايير القوية والفعالة من شــأنه أن يســاعد المؤسســات على كسب المزيد مــن الضمانات المتعلقة بالضوابط الداخليــة وقضايا أمن تقنية المعلومات الخاصة بمقدمي خدمات الحوســبة السحابية. على كل حال فإنه حتى وقت نشر هذا الكتاب لم يكن هناك معايير محددة ومتاحة بشكل علني فيما يتعلق بالحوسبة السحابية.

وفي ظل عدم وجود مجموعة محددة أو معرفة لمثل تلك المعايير، فإنه يجب على المدير الأول أو مدقــق تقنية المعلومــات الذي يقوم بمراجعة التطبيقــات المقدمة من قبل مزود خدمات الحوســبة الســحابية أن يطلب من مزود الخدمة تقديــم ضمانات كافية في ثلاث مجالات رئيسية على الأقل هي:

١- **الأحداث Events:** يجب أن يقوم مزود الخدمة وبشكل منتظم بتوثيق جميع التغيرات، والإبــلاغ عنها وعن غيرها من العوامل الأخرى التي تؤثــر في إتاحة نظام البنية الموجهة نحو الخدمات SOA.

٢- **سجلات Logs:** يجب أن يقوم مزود الخدمة بتقديم معلومات شاملة عن تطبيق البنية الموجهة نحو الخدمات SOA الخاص بالمؤسسة وعن بيئة التشغيل الخاصة به.

٣- **المراقبة Monitoring:** أي عملية رقابية من هذا النوع لا يجب أن تكون تطفلية ويجب أن تكون مقتصرة فقط على الاحتياجات المنطقية الخاصة بمقدم الخدمة الســحابية لكي يقوم بتشغيل مرافقه.

تتيح الحوسبة الســحابية بعضاً من الفرص الجديدة والهامة من أجل إعادة النظر فيما يتعلق بأمن وضوابط تقنية المعلومات من أجل غدٍ أفضل، ولا بد أن يَتْبَع ذلك قريباً معايير ذات طابع أكثر رسمية في ما يخص الحوسبة السحابية. ونستطيع أن نتوقع مشاهدة ما هو أكثر من ذلك بكثير في المستقبل نظراً لأن التطبيقات السحابية والحوسبة السحابية لمزودي الخدمات في نمو ونضوج مستمر.

تحديات الأمن والخصوصية في بيئة الحوسبة السحابية:

إن اســتخدام التطبيقــات التي تعمل في بيئة الحوســبة الســحابية قــد عمل على نقل مجموعة كبيرة من التحديات والمســؤوليات من إدارة تقنية المعلومات الخاصة بالمؤسســة بشــكل أســاسي إلى البيئة التي قد فُرِضت فيها بعض المســؤوليات من قبــل مقدم خدمة الحوســبة الســحابية، في حين لا يزال البعــض الآخر منها من مهــام إدارة تقنية المعلومات الخاصة بالمؤسســة. وهذا هو التحدي بالنسبة لإدارة تقنية المعلومات والمدققين الداخليين التابعــين لها على حد ســواء، والذين يجــب عليهم فهم ومعرفة مكونــات أمن المعلومات والخصوصية التي تخص مقدمي خدمات الحوسبة السحابية الذين اختاروهم بأنفسهم.

لا تزال الحوســبة الســحابية عبارة عــن توجه جديد ومتطور. فعــلى الرغم من العدد المتزايد لمزودي الخدمات الذين يقومون بتقديم خدمات اســتضافة التطبيقات الســحابية، وعلى الرغم أيضاً من وجود مزودي خدمات مثل شركة جوجل وشركة أمازون الذين يقومون ببناء بيئات ضخمة ومعقدة ومتعددة الخوادم للحوســبة الســحابية، إلا أنه لا يوجد هناك مجموعــة محددة لأفضل الممارســات المتفق عليها بين مختلف هــؤلاء المزودين للخدمات الســحابية. في بعض الأحيــان نرى أن هذا التوجه الموجود اليوم لدى المؤسســات لتحويل بعــض مــوارد تقنية المعلومات الخاصة بها إلى مقدمي خدمات الحوســبة الســحابية، ولو بطريقة ربما تكون غريبة بعض الشيء، يشــبه في بعض عنــاصره عملية الانتقال إلى ما كان يعرف باسم مكاتب خدمات تقنية المعلومات والتي ظهرت في أوائل الثمانينيات من القرن الماضي والتي أصبحت الآن من مفاهيم الماضي.

قــررت العديد من المؤسســات في منتصف وحتى نهاية ســبعينيات القــرن الماضي أنها بحاجة إلى الانتقال من عمليات وحدة ســجلات البطاقات المثقبة إلى أحد نظم الحواســيب

المركزيــة mainframe المتطــورة. لذا فقد تم إضافة الكثير من الكــوادر البرمجية المُطَوَرَة للنظم والنظم الحاســوبية المركزية الجديدة التي تم بناؤها وتنفيذها، غير أن النتائج كانت مخيبــة جداً للآمال. حيث كانت المشــكلة المتكــررة هنا هي أن نظم الحوســبة المركزية الجديدة تلك لا تملك السعة الكافية لمعالجة الكميات المطلوبة من بيانات المؤسسات، وفي حال قامت بذلك، كانت تواجة العديد من مشاكل الصيانة والتوقف عن العمل.

وقد كان الحل بالنسبة للعديد من المؤسسات وقتها هو تحويل ونقل عمليات التشغيل الخاصة بنظمهم الحاسوبية إلى ما كان يعرف وقتها بمكاتب الخدمة – وهو أحد أكبر موارد نظم الحاســب المركزية الــذي كان يقوم بتجميع المدخلات للعديد مــن العملاء ومعالجة النظم الخاصة بهم وتسليم تقارير بالمخرجات. ولم تكن مكاتب خدمات النظم الحاسوبية تلك تعمل على نحو جيد أو مناســب بالنســبة للجميع. فقد كان العديد من المشاركات في تلك الخدمات يتم دون إدراك ووعي تام لما سيحصلون عليه من حيث الخدمات وإمكانية المحافظــة على أمن وســلامة معلوماتهم وإمكانيــة متابعة الضوابــط الداخلية للعمليات الخاصة بمؤسساتهم. لقد انتهت عمليات التشغيل الحاسوبية الخاصة بمكاتب الخدمة هذه ولم يعــد لها وجود في هذه الأيام، وكان ذلك حتى قبل زوال الأجهزة المركزية mainframe بفــترة كافيــة. على كل حال فقــد وقعت بعد ذلك بعض الأمور المشــابهة لما يحدث هذه الأيام مع المؤسســات التي تقوم بتحويل بعض عمليات التشغيل الاعتيادية الخاصة بها إلى بيئة الحوســبة السحابية. القضية الرئيسية هي أن المؤسسات لا تقوم دائماً بتوجيه الأسئلة الملائمــة لمقدمي الخدمات الخاصة بهم عندما يقومون بالتحويل إلى البيئة الســحابية ذات البنية الموجهة نحو الخدمات SOA.

عند اتخاذ قرار يتعلق باختيار مقدم الخدمة كجزء أساسي من عملية الانتقال إلى البنية الموجهة نحو الخدمات SOA والحوســبة الســحابية، فإن المؤسسة يجب أن تسأل كلاً من هؤلاء الباعة المتنافســين على تقديم الخدمات بعض الأســئلة الحاسمة والمهمة التي تتعلق بعمليات التشغيل والمعايير الخاصة بهم. ويجب على الفريق الإداري المسؤول عن حوكمة تقنية المعلومات في المؤسســة الحصول على ضمانات كافية بشأن بعض المجالات والمخاوف السبع التالية في عملية مزود الخدمات الحاسوبية السحابية:

١- **المستخدم المصرح له بالوصول إلى البيانات:** إن البيانات الحساسة التي تتم معالجتها خارج المؤسسة وفي بيئة الحوسبة السحابية تحمل معها مستوى متأصلاً من المخاطر، نظراً لأن خدمات التعهيد الخارجي تغفل الضوابط المادية والمنطقية وكذلك الضوابط الخاصة بالأفراد العاملين بتقنية المعلومات التي تمارسها إدارة تقنية المعلومات على برامج نظمها الداخلية وتبذل فيها الكثير من الجهد. لذا يجب على مقدم خدمة الحوسبة السحابية إعطاء معلومات وضمانات كافية تتعلق بالأشخاص الذين سيتولون إدارة بيانات ونظم المؤسسة في البيئة السحابية. كما يجب على مزودي الخدمات توفير معلومات محددة عن عمليات التوظيف والإشراف على مديري النظم أصحاب الامتيازات والصلاحيات وعن الضوابط المفروضة على وصولهم للبيانات والنظم.

٢- **الامتثال التنظيمي:** إن المؤسسة في النهاية هي المسؤولة عن أمن وسلامة بياناتها حتى بعدما تقوم برفعها إلى أحد مزودي الخدمات. لذا يجب على مقدم الخدمات الحاسوبية السحابية إعطاء معلومات تفصيلية وكافية عن السياسات الخاصة بحوكمة الأمن المتبعة لديها وعن النتائج المعلنة الخاصة بتقارير عمليات التدقيق الخارجي الأخيرة وبالشهادات المتعلقة بالأمن لديه. ويجب أن يوافق مزود الخدمة على إخطار المؤسسة بتلك الأنشطة بشكل منتظم.

٣- **أماكن البيانات:** عندما تقوم المؤسسة باستخدام البيئة السحابية لتخزين البيانات والنظم الأساسية الخاصة بها، فمن المحتمل ألا تكون المؤسسة على علم بالمكان الذي سيستضيف البيانات الخاصة بها، بل حتى بالدولة التي ستوجد بها هذه البيانات والنظم. وبموجب قوانين ملكية البيانات، فإنه يتعين على مقدمي خدمات الحوسبة السحابية تقديم معلومات كافية عن الالتزامات والاختصاصات القضائية للأماكن التي سيتم فيها حفظ ومعالجة بيانات المؤسسة. كما يجب على مقدم الخدمة أيضاً إبرام عقد إلزامي بالامتثال والالتزام بمتطلبات الخصوصية المحلية نيابة عن عملائه.

٤- **الفصل بين البيانات:** تكون البيانات عادة داخل السحابة في بيئة مشتركة بجانب بيانات خاصة بعملاء آخرين. لذا يجب على مقدم الخدمة توفير معلومات تفصيلية حول ما سيتم عمله لفصل البيانات في فترات التوقف، ويجب عليه أيضاً تقديم دليل يُثْبِت أن

برامج التشــفير الخاصة به قد تم تصميمها وفحصها من قبل خبراء مختصين. فحوادث التشــفير قد تجعل البيانات غير صالحة للاستعمال بشكل كامل، بل من الممكن أيضاً أن تجعل حتى إتاحتها عملية صعبة ومعقدة.

٥- **اســترجاع البيانــات:** حتى إن كانت المؤسســة لا تعلم المكان الذي توجــد فيه بياناتها داخل الســحابة، فإنه يجب على مزود الخدمات الســحابية أن يقوم بتوثيق ما سيحدث لبيانــات وخدمات المؤسســة في حال وقوع الكوارث. كما يجــب عليه أن يقدم الدليل، متضمناً نتائج الفحص الخاصة به، والذي يثبت أن وسائل الاسترجاع والتعافي المستخدمة لديه قادرة على عمل نسخ طبق الأصل من البيانات والبنية التحتية للتطبيقات عبر عدة مواقع. كما يجب على الخدمة أن تؤكد ما إذا كانت لديها المقدرة على إجراء الاستعادة الكاملة وكم من الوقت ستأخذ للقيام بذلك.

٦- **دعم التحقيق والاســتقصاء:** قد يكون من المســتحيل حدوث أنشــطة تخص التحقيق أو الاســتقصاء غير الملائم أو غير القانوني في الحوســبة السحابية. حيث إنه من الصعب إجراء تحقيقات أو استقصاءات تتعلق بالخدمات السحابية على وجه الخصوص نظراً لأن عملية الدخول وكذلك البيانات للعديد من المستخدمين قد تتشارك في الموقع وقد تنتشر أيضــاً عبر مجموعة من الخوادم المضيفة ومراكز البيانات الدائمة التغيير. لذا يجب على مقدم الخدمة إبرام عقد إلزامي لدعم أشــكال محددة من التحقيقات والاســتقصاءات، إلى جانب تقديم الدليل على أن مقدم الخدمة بالفعل قد قام بدعم مثل هذه الأنشطة بنجاح.

٧- **قابلية الاستمرار والتطبيق لفترة طويلة:** لا يوجد لدى المؤسسة أي ضمانات بأن مقدم خدمة الحوســبة السحابية الخاص به لن ينكسر أبداً أو يتم ابتلاعه والاستحواذ عليه من قبل شركة أكبر. على كل حال فإنه يجب على المؤسسة أن تحصل على ضمانات كافية من مقدم خدمة الحوسبة السحابية الخاص بها بأن بياناتها ستبقى متاحة حتى بعد حدوث ذلك. كما يتعين على أي مقدم خدمة تقديم الضمانات الكافية بأن المســتخدمين سوف يسترجعون بياناتهم وبالصيغة التي تسمح لهم باستخدامها في التطبيقات البديلة.

تعد الحوسبة السحابية وتطبيقات البنية الموجهة نحو الخدمات SOA الخاصة بها من المجالات المتطورة والسريعة التغير. لذا فإننا نستطيع أن نتوقع رؤية المزيد من المعايير الموضوعة وأفضل الممارسات المتعارف عليها في المستقبل. وعلى الرغم من أننا قد أشرنا إلى مكاتب خدمات تقنية المعلومات التي كانت تستخدم منذ سنوات عديدة مثالاً على كيفية عدم اختيار مقدم الخدمات السحابية، فإننا نشعر بأنه كان هناك ما يكفي من الدروس المستفادة في هذا الصدد لعدم تكرار مثل تلك الأخطاء. فالحوسبة السحابية هي الموجة المستقبلية، ويجب علينا أن ننظر إلى المزيد من الاستخدامات لهذا المفهوم في السنوات القادمة.

نظم تقنية المعلومات وافتراضية إدارة التخزين:

الافتراضية هي مفهوم يعبر عن تجميع وسائل التخزين المادية لتقنية المعلومات من عدة أجهزة تخزين شبكية داخل ما يبدو وكأنه وحدة تخزين واحدة يتم إدارتها من خلال وحدة تخزين مركزية. حيث يساعد التخزين الافتراضي المدير المسؤول عن التخزين في تقنية المعلومات على إنجاز مهام النسخ الاحتياطي والأرشفة واسترجاع البيانات بشكل أكثر سهولة وفي وقت أقل، وذلك عن طريق إخفاء التعقيدات الحقيقية الموجودة في شبكة أجهزة تخزين تقنية المعلومات بالكامل. وقد قدم مؤلف هذا الكتاب لافتراضية إدارة التخزين لأول مرة عام ٢٠٠٢ عندما كان عضواً في مجموعة استشارية صغيرة في شركة إي إم سي EMC التي قامت بإطلاق الممارسات الاستشارية لمكتبة البنية التحتية لتقنية المعلومات Information Technology Infrastructure Library (ITIL) (وقد تم مناقشة أفضل الممارسات المتعلقة بآيتل في الفصل السادس من هذا الكتاب). في هذا الوقت، كانت شركة EMC أحد الرواد في مجال أجهزة إدارة التخزين وكان تقديمها لمفاهيم الافتراضية يعد ابتكاراً تقنياً كبيراً. وقد أصبحت الافتراضية منذ ذلك الوقت تُستخدم على نطاق واسع كما أنها إحدى العمليات الهامة لإدارة موارد تقنية المعلومات.

ولفهم ومعرفة افتراضية تقنية المعلومات، ينبغي على المرء أن يعود مرة أخرى إلى الأيام الأولى للنظم الحاسوبية - ولاسيما الأجهزة المركزية الكبيرة mainframes التي كانت تستخدم في الماضي. فقد كانت أنظمة التشغيل لتلك الحاسبات تتحكم

في مجموعــة مختلفة من الأجهزة الطرفية المتصلة، متضمناً ذلك الطابعات ومشــغلات الأشرطة وما كان يطلق عليه وقتها قرص التخزين الضخم وأجهزة تشــغيل الأسطوانات. وعلى الرغم من أن أنظمة الحاســبات المركزيــة mainframe البدائية هي التي قامت في البداية بالاســتخدام المكثف لمشــغلات الأشرطة الممغنطة الرخيصة نسبياً في عمليات تخزيــن البيانات؛ فــإن التقنية سرعان ما تحولت إلى اســتخدام أجهــزة التخزين التي اعتمدت في البداية على الأســطوانات الممغنطة الدوارة ومن ثم على مشغلات الأقراص. وعلى الرغم من الأثمان الباهظة لمشغلات الأسطوانات والأقراص عندما تم تقديمها لأول مرة في الأيام الأولى لظهور تقنية المعلومات، فإنه سرعان ما أصبحت تلك المشغلات أكثر شيوعاً واستخداماً من مشغلات الأشرطة البدائية. فقد كانت مشكلة مشغلات الأشرطة هي أنه من أجل قراءة الســجل رقم ١٠٠,٠٠٠ مثلاً لابد أن يمر مشغل الشريط أولاً على ٩٩،٩٩٩ ســجلاً قبله للوصول إليه. وسرعان ما أصبحت مشــغلات الأســطوانات بمثابة بصمة تاريخيــة، وسرعان ما انتقلت التقنية إلى الأقراص الــدوارة التي امتازت بالسرعة العالية وبمخططات الفهرسة التي كانت تسمح لها بتحديد موقع السجل رقم ١٠٠,٠٠٠ بشكل فوري إلى حد ما.

بوجه عام، فإن افتراضية تقنية المعلومات تعني إنشــاء نســخة افتراضية من أجهزة أو موارد تقنية المعلومات، مثل الخادم، أو أجهزة التخزين، أو الشبكة، أو حتى نظام التشغيل حيــث يعمــل إطار العمل على توزيع هــذا المورد على واحد أو أكثر من بيئات التشــغيل. حتى إن الممارســة الشــخصية الشــائعة والخاصة بتقســيم القرص الصلب لنظام الحاسب المكتبي (الشــخصي) تعد شــكلاً من أشــكال الافتراضية نظراً لأنك تقــوم بأخذ قرص واحد وتقوم بتقســيمة إلى اثنين من مشــغلات الأقراص الصلبة. حيث يستطيع كل من الأجهزة والتطبيقــات والمســتخدمين التفاعل مع هــذا المورد الافتراضي كما لــو كان مصدراً منطقياً واحــداً حقيقياً. لقد أصبح مصطلــح الافتراضية بطريقة ما مصطلحاً شــائعاً في عالم تقنية المعلومات، وأصبح يُطلق على نظم الحاسب والعناصر التي تم تحويلها إلى البيئة الافتراضية اســم الأجهزة الافتراضيــة Virtual Machines (VMs). ترتبط افتراضية تقنية المعلومات بعدد من التقنيات الخاصة بتقنية المعلومات تشمل ما يلي:

- **التخزيــن الافتراضي Storage virtualization:** وهو دمج العديد من أجهزة التخزين الشــبكي بحيــث تبدو كأنها وحدة تخزيــن واحدة، فقد كانت المــرة الأولى التي تم فيها تقديــم افتراضية إدارة التخزين لتقنيــة المعلومات نحو عام ٢٠٠٢ من قِبل شركة EMC، وقد تم التقاط هذا المفهوم من قِبل العديد من بائعي المعدات الحاســوبية لنظم إدارة التخزين.
- **الخــادم الافــتراضي Server virtualization:** وهو تقســيم الخــادم الفعلي إلى خوادم افتراضيــة أصغر حجماً. وقد كانت شركة IBM هي أول من طور هذا المفهوم عن طريق نظام التشــغيل الخاص بالحاسب المركزي الافتراضي VM mainframe الخاص بها والذي يعود إلى ثمانينيات القرن الماضي.
- **نظام التشغيل الافتراضي Operating system-level virtualization:** وهو أحد أنواع التقنية الافتراضية للخادم التي تتعامل مع نظم التشغيل المعقدة ذات الطبقات البرمجية المتعددة.
- **الشــبكة الافتراضية Network virtualization:** يمكن جعل الشــبكة الفعلية الواحدة عبارة عن شبكة افتراضية من خلال عمليات التقسيم المنطقية لموارد الشبكة.
- **التطبيق الافتراضي Application virtualization:** يمكن اســتخدام هذا المفهوم نفسه لزيادة فائدة وكفاءة تقنية المعلومات وإدارة عمليات الترقية والنســخ الاحتياطي بصورة أكثر سهولة. وهو ما سنقوم بتوضيحه في القسم التالي.

إن الافتراضية عموماً هي فصل وظائف الجهاز عن عناصره الحقيقية باستخدام برمجيات خاصة. ففي البيئة الافتراضية يتم فصل الموقع الفعلي للوحدة عن وظائفه وتقوم برمجيات التحكــم بإدارة البيانات أو الوظائف بغض النظر عن أماكنها الحقيقية. حيث تعتبر عملية إدارة وحــدات مادية منفصلة والتحكم بها من خــلال برنامج خاص بالافتراضية من الطرق الفعالة جداً. فباستخدام برمجية التحكم المناسبة، يمكن استخدام تقنيات البيئة الافتراضية في العديد من أجهزة ومعدات تقنية المعلومات متضمنة إدارة التخزين ومكونات الشــبكة والخوادم وأنظمة التشغيل وحتى التطبيقات.

لقد اقتحمت اليوم البيئة الافتراضية لتقنية المعلومات صناعة تقنية المعلومات بكل ما تعنيه الكلمة من معنى. فقد أشارت استطلاعات الرأي إلى أن ما يزيد عن نصف إدارات تقنية المعلومات في المؤسسات الكبيرة حالياً تقوم بتشغيل خادم افتراضي واحد على الأقل، وأن هناك عدداً أقل بكثير لكن متزايد من هذه الإدارات لديها إستراتيجيات أمنية قد صُممت خصيصاً للعمل في تلك البيئة الافتراضية الخاصة بها. من ناحية أخرى، سواء كانت المؤسسة قد قامت فعلاً بتطبيق إستراتيجية البيئة الافتراضية لتقنية المعلومات أم ما زالت في طور التطبيق لها، فمن المحتمل أن تكون الشركة عرضة لمخاطر التهديدات الأمنية التي يمكن أن يكون لها تأثير كبير في البيئة التشغيلية الخاصة بالمؤسسة. ولما كانت النظم التقليدية لأمن تقنية المعلومات تعتمد على المعدات وعلى نظم التشغيل الخاصة لتقوم بحماية البيئة التي تعمل بها، فإنها تكون عديمة الفائدة في البيئة الافتراضية التي تهدف بالأساس إلى تقليل المعدات المستخدمة أو الاستغناء عنها.

هذا بالإضافة إلى أن أفضل الممارسات التقليدية أصبحت الآن في موضع شك نظراً لأن تنفيذ التجزئة المادية وغيرها من الأساليب الأخرى يعد أمراً مستحيلاً إلى حد ما في ظل تلك الممارسات. وأخيراً، فإنه نظراً لطبيعة البيئة الافتراضية، تتزايد تعقيدات الشبكة بشكل أسرع من نظم الإدارة والمراقبة القديمة، مما يجعل الرؤية فيما يتعلق بالبيئات الافتراضية والحقيقية غير واضحة تماماً. لذلك تحتاج المؤسسات إلى أن تنظر بعمق إلى الأساليب الجديدة المتبعة لتأمين شبكاتها ومعلوماتها الحساسة في العالم الافتراضي الجديد.

يناقش القسم التالي بعض القضايا الفريدة الخاصة بأمن تقنية المعلومات والمرتبطة بتطبيق البيئة الافتراضية لتقنية المعلومات، التي تتجاوز القضايا العامة لحوكمة أمن تقنية المعلومات والتي تمت مناقشتها في الفصل العاشر من هذا الكتاب. بالإضافة إلى ذلك قد تثير البيئة الافتراضية بعض القضايا الفريدة لحوكمة تقنية المعلومات. لذا يتعين على المديرين فهم إستراتيجية البيئة الافتراضية وعمليات الرقابة الداخلية لإدارات تقنية المعلومات الخاصة بهم.

حوكمة تقنية المعلومات والافتراضية:

كـما ذكرنا سـابقاً، كان الظهـور الأول لمفهـوم الافتراضية في عصر الحاسـبات المركزية mainframe عندمـا قامت شركـة IBM بطرح المفهوم الذي أطلقت عليه اسـم الأجهزة الافتراضية VM Machines كأحد العناصر الخاصة في بنية الحاسـبات المركزية لديها، وقد كان ذلـك في ثمانينيات القـرن الماضي. ثم انتقلـت الخصائص الفريـدة الخاصة بالأجهزة الافتراضية بعد ذلك إلى حاسبات سطح المكتب، تماماً كما انتقلنا نحن إلى النظم القائمة على بيئـة الخادم-العميل ثم انتقلت إلى عالم الإنترنت. لقد أصبحت الافتراضية اليوم في مقدمة الموضوعات الساخنة نظراً لأننا نقوم بتحويل عمليات إدارة التخزين من البيئة الواقعية إلى الافتراضيـة وتطبيق الأجهزة الافتراضية في بيئة النظم الشـبكية المتعددة الخوادم الموجودة اليوم.

لقد اعتقد مديرو مراكز البيانات بداية بأنهم يسـتطيعون إدارة تلك الأجهزة الافتراضية بطريقة تشـبه كثيراً الطريقة التي يستخدمونها في إدارة الخوادم الحقيقية الخاصة بهم، إلا أن التجربة أثبتت استحالة هذا الأمر بشكل عام. فمع وجود العديد من القواسم المشتركة بين البيئتين الافتراضية والحقيقية، هناك أيضاً بعض الاختلافات الجوهرية التي تؤثر في إدارة وحوكمة النظم.

إن التأثـير المحتمل لافتراضية إجراءات وعمليات الرقابة الموجـودة والمعمول بها حالياً يعد واحداً من الاختلافات الرئيسـية الكبيرة هنا. فعلى سـبيل المثال، هناك مجموعة من العمليـات والإجراءات المتبعة في مركز البيانات بخصـوص عملية إضافة وتجهيز مجموعة من الخوادم الجديدة، ويتضمن ذلك سلسـلة من التوقيعات والإجراءات المتعلقة بعمليات التسـليم الموجودة بين مختلف فرق مركز البيانات، وينتج عن ذلك في النهاية خادم جديد تم تركيبه في مركز البيانات. فضلاً عن إمكان إحدى عمليات تشغيل تقنية المعلومات إنشاء خـادم افـتراضي جديد، حرفياً، بمجـرد النقر على زر الفأرة - وذلك إما بنسـخ أحد الأجهزة الافتراضية الموجودة أو إنشاء جهاز افتراضي جديد من القوالب المخصصة لذلك - وقد أصبح من السهل تجاوز مثل تلك العمليات.

على سـبيل المثال يمكن لعمليات تشـغيل تقنية المعلومات المؤسسـية عمل عدة نسخ افتراضية متماثلة من الخادم نفسـه وتوزيعها على وحدات التشـغيل الموجودة في المنظمة المحيطـة بها. وقد تكون هناك تحديات بالنسـبة للحوكمة والرقابة في تتبع هذه النسـخ. حيث سـتقوم النظم الإدارية المقدمة من قبل بائعـي البرمجيات الافتراضية بتحديد أماكن الأجهزة الافتراضية عند لحظة زمنية محددة، ولكنها عاجزة عن أن تحدد أين كانت أو مدى علاقتها بالخوادم الافتراضية الأخرى. ومما يزيد الأمر تعقيداً حقيقة أن الأجهزة الافتراضية، كـما تم تعريفهـا، متحركة. فهي قادرة عـلى الحركة حول البيئة الخاصـة بها بعد أن يتم نشرهـا. فهـذه الحركة لا تجعل عمليـة تتبع وإدارة تلك الأجهـزة الافتراضية أكثر صعوبة فحسب، بل يمكن أيضاً أن تكشف السياسات الخاصة بتقسيم البيانات والتطبيقات.

إن هذه الاختلافات، وغيرها، تجعل من الصعب أيضاً بالنسبة لمعظم أدوات إدارة مراكز البيانات المعمول بها حالياً أن تكون قادرة على العمل في الفضاء الافتراضي وسـترك العديد مـن النقاط المبهمة أو الغامضة. ومما يزيد هذا الأمـر تعقيداً قلة الأدوات اللازمة للإدارة الافتراضيـة وإعداد التقارير الخاصة بها وأتمتها. وتكـون النتيجة بيئة يدوية تماماً حيث لا تتكامـل على نحو جيد مع نماذج الامتثال والرقابة الحاليـة لمركز البيانات. وهذا يعني أن نظم "الراية الحمراء" أو التنبيه التقليدية قد لا تتمكن من العمل بالشكل المناسب في هذا الفضـاء (الافتراضيـة)، فهي إما أن يتم التحايل عليها وإما أنها ببسـاطة لا تسـتطيع رؤية عمليات التشغيل اليومية، فتترك مراكز البيانات مكشوفة أو مستهدفة.

في مركز البيانات الفعلي الخاص بتقنية المعلومات وبجميع ما يتضمنه من نظم وعمليات وضوابط وتوازنات رقابيـة، يتم إصدار التنبيهات في حال حدوث أمور خارجة عن المألوف. فالإدارة ومن خلال الاسـتثناء تكون هي القاعدة المتبعة اليوم وهي البيئة التي تعتبر عدم وجود أخبار جديدة هو بحد ذاته خبراً جيداً. لكن البيئة التي تكون فيها الضوابط اليدوية هي المهيمنة غالباً وتشح فيها عمليات التبليغ عن الأحداث، وقصور الرؤية الرقابية قد تؤدي إلى إيجاد قضايا لن تسـتطيع إدارة عمليات تشـغيل تقنية المعلومات التنبؤ بها مسـتقبلاً. وقد لا تعد قضية ضخمة بالنسبة لبيئة الحوسبة الافتراضية الصغيرة، ولكن كلما نمت البيئة وازداد حجمها، نمت معها أيضاً آثار تلك القضايا.

عندما تقوم إدارات تقنية المعلومات المؤسسية بتبني تلك البيئات الافتراضية، فإن نقص الضوابــط الآليــة في بعض بيئات الأجهــزة الافتراضية والحاجة المتزايدة لأنشــطة الضوابط الداخلية اليدوية قد يتسبب في حالة من عدم التوازن بين عمليات التشغيل الخاصة بتقنية المعلومــات وعمليات التشــغيل الخاصة بالضوابط الداخلية. وســوف تتفاقم هذه الحالة (حالة عدم التوازن) فقط عندما تنمو بيئة الأجهزة الافتراضية. إن هذا النقص في الضوابط الآلية، والمتابعة، والقياس المســتمر في مراكز البيانات الافتراضية، إضافة إلى زيادة العمليات اليدوية المصاحبة، أدى إلى اســتحداث بيئة تحتــوي على ضوابط ذات فاعلية أقل ومخاطر أكثر من البيئة الحقيقية المناظرة لها.

قضايا حوكمة وأمن البيئة الافتراضية لتقنية المعلومات:

عندما ينتقل التخطيط الذي يُبذل فيه جهد كبير ولكنه في النهاية يخرج بشــكل ســيئ إلى البيئة الافتراضية، فإنه قد يتســبب في إيجاد تحديات بالنســبة للمؤسسة. وكما ناقشنا في الفصــول الأخرى، كلما خرج المزيد مــن الأنظمة الموضوعة للحوكمــة، وإدارة المخاطر، والامتثــال (GRC) عــن التــوازن، زاد التأثير في الأعمال بصورة كاملــة. إن "نقاط التحول" الفردية هنا ســتكون مختلفة لكل مؤسســة على حدة، ولكن عاجلاً أو آجلاً سيتم الوصول إليها، وذلك عندما تبدأ المؤسســات في رؤية التصاعد المستمر في تكاليفها ومخاطرها. وربما يكون هناك العديد من المؤسســات التي تعمل حالياً في ظل وجود نفقات غير مخطط لها على تقنية المعلومات، وذلك بســبب انتقالها إلى بيئات افتراضية غير فعالة. في حين تشــهد مؤسســات أخرى ارتفاع نسبة الحوادث المرئية وغير المرئية في مراكز البيانات. جميع هذه الأمور ستؤثر في نهاية المطاف على مجمل أداء الأعمال المؤسسية.

ينبغي على المدير الأول في المؤسســة أن يناقش إستراتيجيات البيئة الافتراضية والأجهزة الافتراضيــة لتقنية المعلومات مع إدارة تقنية المعلومات. فــإذا بدا أن الانتقال إلى الأجهزة الافتراضية سيكون على النحو المتفق عليه، فإنه يجب أن يكون هناك دليل على وجود خطة قوية لهذا المشروع (مشروع الانتقال)، كما تمت مناقشــته في الفصل السادس عشر من هذا الكتــاب، هذا بالإضافة إلى وجود تقدير واضح لبعض المخاوف الاســتثنائية للرقابة المرتبطة بالبيئــة الافتراضية لتقنيــة المعلومات. ولا يزال هناك العديد من السياســات التشــغيلية

وسياسات المخاطر والأهداف الرقابية يمكن تطبيقها في العالم الافتراضي. ربما يكون قد تم ضبطها لتتناسب مع الطبيعة الحركية لتلك البنية الجديدة، لكنها لا تزال تُطبق. وذلك يشمل العناصر المشتركة بالنسبة لجميع الخوادم (حقيقي أو افتراضي) كالتهيئة، وإدارة التوصيلات (التوصيلات الكهربائية)، والأمن. من ناحية أخرى، فإن للبيئة الافتراضية تفردياً يتطلب سياسات وضوابط جديدة تشمل ما يلي:

- **إدارة الهوية Identity management:** نظراً للطبيعة الحركية للأجهزة الافتراضية، ستكون هناك حاجة إلى مستوى ما لإدارة هوية الملفات والموارد التي لا تعتمد على (الأعراف) البسيطة للتسمية. لذا يتعين على وحدة ضمان جودة تقنية المعلومات إلى جانب التدقيق الداخلي لتقنية المعلومات، مراجعة وتقييم العمليات من أجل ضمان تطبيق السياسات بشكل سليم.
- **التحكم في تنقلية الجهاز الافتراضي VM mobility control:** أحد العناصر الأساسية في القيمة المضافة بالنسبة للبيئة الافتراضية هو المرونة التي قدمتها لمجموعات تقنية المعلومات. فقد تم تصميم الأجهزة الافتراضية بحيث تكون متحركة وتستطيع بكل سهولة الانتقال من خادم إلى آخر، سواء كان ذلك استجابةً للعمليات الآلية لتوازن الأحمال، أم بسبب الإزالة اليدوية للأجهزة الافتراضية من أحد الخوادم الحقيقية التي تحتاج إلى صيانة. من ناحية أخرى، فإن هذه المرونة يمكن أن تكون سلاحاً ذا حدين، وذلك عندما لا يجب أن تكون جميع الأجهزة الافتراضية متنقلة. فعلى سبيل المثال، قد تحتاج إدارة تقنية المعلومات، سواء لأهداف تتعلق بالرقابة أم بالتدقيق، إلى إثبات أن تطبيقاً ما متفق مع اللوائح التنظيمية أو المعايير الداخلية للشركة. فربما يكون هناك حاجة لسياسات تتعلق بالأماكن التي يجب والتي لا يجب أن تعمل بها بعض الأجهزة الافتراضية المحددة، كما تتعلق أيضاً بتحديد المدة الزمنية التي يُسمح بها ببقاء الأجهزة الافتراضية دون اتصال.
- **التزويد الاحتياطي Provisioning:** يمكن التحايل بسهولة على العمليات التقليدية المتبعة لإضافة خادم جديد. لذا لا بد من وضع عمليات جديدة تحكم كلاً من: ما الذي سيتم التزود به؟ (ما الذي سيتم إنشاؤه احتياطياً؟)، ومن الذي يملك سلطة السماح بإضافة خوادم جديدة؟

- **فصــل البيانــات Data separation:** لكل مركز بيانات مجموعة مــن القواعد المتبعة للقيــام بعملية الفصل بــين بيانات التطبيقات لديــه، والتي يكون الدافــع لها عادة إما المخاوف الأمنية أو القضايا المتعلقة بالامتثال. فعندما تقوم إدارة تقنية المعلومات بوضع التطبيقــات في البيئة الافتراضية والتي تندرج تحت هــذه المعايير، فمن المهم التفكير في الكيفيــة التي ســيُفرض بها هذا الأمر عــلى الجانب الافتراضي، ولكن أيضــاً للحماية من التحركات غير الملائمة المقصودة وغير المقصودة خلال دورة حياة هذا الخادم.
- **الاســترداد Reclamation:** إن ضمان إزالة الأجهزة الافتراضية الزائدة أو غير المستخدمة يعــد مجالاً آخر من المجالات التي تتطلب سياســة وأهدافاً معينة. كما أن الآثار الأمنية المترتبــة على هذه التقنية الجديــدة هي أيضاً بحاجة إلى أن تؤخــذ بعين الاعتبار، وهي تشــمل: تأثير الأجهزة الافتراضية على النظم الأمنية لتقنية المعلومات المعمول بها حالياً (فبعــض النظم لا تعمل جيداً في البيئة الافتراضية)، ومــدى احتمالية التعرض لتهديدات هجومية جديدة.

قد لا يكون المدير التقليدي المســؤول عن حوكمة تقنية المعلومات المؤسســية مُلماً بتلك القضايا والمســائل الســابقة الذكر. ومع ذلك، قد تُســتخدم تلك المسائل نقاط حوار رئيسية خــلال الحديث مع إدارة تقنيــة المعلومات لديهم حول ما يتعلــق بتقييم أي برنامج يخص افتراضية تقنية المعلومات داخل المؤسســة. وعلى الرغم من سرعة تبني الخادم الافتراضي في جميع أنحاء العالم، فإنها لاتزال تقنية غير ناضجة نسبياً. فبالنسبة للكثيرين قد دخل الخادم الافــتراضي إلى مركز البيانات من الباب الخلفي كأحد الأدوات التشــغيلية المســتخدمة والتي حققت مســتوى جيداً مــن العوائد الاســتثمارية (Return On Investment (ROI، وقد تطور الخادم الافتراضي منذ ذلك الوقت ليصبح البنية الهيكلية الجديدة لمركز البيانات. لكن دخوله بهــذه الطريقة جعله لا يخضع أبداً للعمليات الاعتياديــة الخاصة بمراجعة الضوابط الداخلية التي يتم اتباعها عادة من قبل إدارات تقنية المعلومات قبل إطلاق الخوادم في مركز البيانات، وأســهم دخول الخادم الافتراضي بهذه الطريقــة أيضاً في نقص بعض الوظائف التي تشتد الحاجة إليها.

يوجد في الســوق اليوم عدد من منتجات منصات البرمجيــات الافتراضية ، وتعتبر في إم وار VMware هي الشركة الرائدة في هذا المجال، مع وجود عدد قليل من الشركات الأخرى مثــل شركة مايكروســوفت Microsoft وشركة ســيتركس Citrix. فلــكل منصة من هذه المنصات مجموعة مختلفة من نقاط الضعف ونقاط القوة، وقد خلصت العديد من إدارات تقنيــة المعلومات إلى تشــغيل خليط مكون من تلك المنصات الثلاث معــاً، الأمر الذي أثار قضية أو مشكلة تتعلق بكيفية إدارة تلك البيئات غير المتجانسة. فليس بالأمر المفاجئ أن تركز نظم الإدارة المُقدَمة من قِبل باعة النظم الافتراضية على نقل الجهاز الافتراضي أكثر من تركيزها على إدارة البيئة نفســها. إضافة إلى ذلك فإن معظم باعة النظم التقليدية الخاصة بــإدارة مراكز البيانات يملكون نظماً تم بناؤهــا للعمل في بيئة مراكز البيانات الحقيقية ولا تعمل جيداً في البيئات الافتراضية.

واعتــماداً على عمليات تشــغيل تقنيــة المعلومات وعلى العمليــات الخاصة بالحوكمة وإدارة المخاطــر والامتثــال GRC التي تمت مناقشــتها في فصول أخــرى، فإنه ينبغي على إدارة المؤسســة العمل مع عمليات تشــغيل تقنيــة المعلومات لديها لمعرفــة ما إذا كانت المعايير المناسبة الخاصة بالرقابة الداخلية لا تزال موجودة ومعمولاً بها في البيئة الافتراضية. فبالنسبة للكثيرين ربما يكون هناك حاجة لنظم إضافية في مراكز البيانات الافتراضية، سواء كان ذلك لتعويض القصور الموجود في نظم إدارة مراكز البيانات والبيئات الافتراضية المعمول بها حالياً أم لفرض وتطبيق سياسات إضافية يتطلبها هذا المجال.

لقــد وُجِدت البيئة الافتراضية هنا لتبقى. لذلــك إذا كثفت إدارة تقنية المعلومات من تبنيهــا للخوادم الافتراضية في مركــز البيانات الخاصة بها، فإنه يجــب عليها أن تأخذ بعين الاعتبار آثار استخدام تلك الخوادم الافتراضية على الضوابط الداخلية للأعمال والتي تتضمن ما يلي:

- **تطبيــق المعايــير والعمليات المعمــول بها حالياً في الفضاء الافــتراضي أينما أمكن:** من المحتمل أن تحتاج المعايــير والعمليات المعمول بها حالياً إلى تعديلات، ولكن مع التأكيد على وضعها موضع التنفيذ لتبدأ بتقديم الرؤية والرقابة المطلوبة بالإضافة إلى التبصر فيما هو ضروري ومطلوب من نظم إدارية إضافية.

- **وضع المعايير والعمليات الجديدة التي تحتاج إليها تلك التقنية:** ينبغي على المؤسسة أن تزيد من مستوى رقابتها إلى ما هو أبعد من ذلك، وعلى الأقل يجب أن تشتمل هذه الأمور على:
  - المراقبة والتبليغ.
  - التحكم في التزويد التقني.
  - إدارة هوية الجهاز الافتراضي.
  - ضبط تنقلية الأجهزة الافتراضية لفرض الفصل بين البيانات.
  - إصلاح الأجهزة الافتراضية عند انتهاء العمر الافتراضي لها.
- **الأتمتة قدر الإمكان:** إن العمليات اليدوية ليست متناغمة وتحتاج إلى المزيد من الوقت لإتمامها. لذا سنجد في نهاية المطاف أن الطريقة الوحيدة لإعادة التوازن لنموذج الحوكمة وإدارة المخاطر والامتثال GRC هو زيادة مستوى التشغيل الآلي عن طريق تطبيق نظم إضافية جديدة يحتاج إليها هذا المجال. وهذا سيكون له تأثير إضافي من أجل الحد من النشاط والعمليات اليدوية، وزيادة الضوابط الداخلية، وتقليل المخاطر، إضافة إلى توفير كميات كبيرة من الوقت المستهلك في العمليات الإدارية.
- **مراجعة البنية الأمنية لديك:** لكي نكون أكثر كفاءة وفاعلية، فإن العديد من أنواع الأجهزة الأمنية والأدوات الرقابية التي نود أن نعرف ما الذي تقوم بحمايته هذه الأجهزة وأين يكون، وكذلك حركة الأجهزة الافتراضية؛ كل ذلك قد يكون محل جدال. وقد يفرض التغيير المستمر الموجود في البيئة الافتراضية مطالب حيوية ديناميكية على أي نوع "ثابت" من أنواع الحلول الأمنية وحتى في البنى التحتية للبيئات الافتراضية الصغيرة. خلاصة القول هي: أن بعض البنى التحتية الأمنية لن تعمل جيداً في البيئة الافتراضية، وربما يكون المنتج الأمني، غير القادر على العمل جيداً على مستوى جميع الأهداف والممارسات، غير قادر أيضاً على العمل مطلقاً.
- **تطبيق معايير تدقيق ومعايير داخلية محددة (ونظم إبلاغ) تناسب الفضاء الافتراضي:** فكما وضحنا سابقاً، إن البيئة الافتراضية تحتاج إلى سياسات وممارسات ومعايير رقابية

جديدة. وعند دخولها حيز التنفيذ، ستحتاج أيضاً إلى رقابة داخلية، وعمليات تدقيق، وإجراءات جديدة مناظرة لها. فعلى سبيل المثال، تحتاج التطبيقات الممتثلة لقانون SOx إلى أن تكون مفصولة عن النظم الأخرى، وتحتاج أيضاً إلى تطبيق ضوابط أكثر صرامة على عمليات الوصول للبيانات. إلا أن التنقلات الطبيعية للخوادم الافتراضية أسهمت في إضافة عامل جديد إلى عملية التدقيق وهو: هل تم انتقال هذا الجهاز الافتراضي إلى أحد الخوادم الإضافية خلال الفترة الزمنية المخصصة لعملية التدقيق؟ إذا كان هذا قد تم، فما الأجهزة الافتراضية الأخرى التي كانت موجودة على هذا الخادم؟

وكما يحدث عادة مع أي تقنية جديدة تخص تقنية المعلومات، قد يتسبب تركيب برمجيات البيئة الافتراضية وكذلك التغييرات الكبرى في إحداث بعض التحسينات الجوهرية على مستوى كفاءة العمليات. على أي حال، فإن إدارة تقنية المعلومات هي من تقوم غالباً بتنصيب تلك الأدوات الجديدة، غير أنها تتجاوز غالباً مستوى فهم الإدارة العامة العليا، لذا يجب أن يحصل كبار المديرين، على جميع المستويات، على فهم عام حول نشاطات البيئة الافتراضية في مؤسساتهم.

يوضح الشكل التوضيحي (٩-٢) قائمة ببعض الممارسات الجيدة لحوكمة تقنية المعلومات في البيئة الافتراضية لإحدى المؤسسات التجارية التقليدية. إذ يجب أن تساعد هذه الممارسات المدير الأول على فهم الكيفية التي من خلالها يتم تطبيق البيئة الافتراضية في المؤسسة.

لقد بدأ العمل بالبيئات الافتراضية في معظم مراكز البيانات على أنه جهد تخطيطي، قاده قسم تقنية المعلومات، وقد ركز وقتها على مسألة الفوائد العائدة من الاستثمارات ROI الخاصة بعملية دمج الخوادم. لكن الانتقال من تكامل الخوادم الذي كان يتم لتحقيق غرض معين إلى البيئة الافتراضية أدى إلى المزيد من الاستخدامات في بيئة العمل الإنتاجية، وزيادة نسبة مراكز البيانات ذات البيئة الافتراضية، كل ذلك يتطلب نظرة أكثر إستراتيجية حول مدى تأثير هذه البنية في إدارة مراكز البيانات والضوابط الخاصة بالأعمال. فوجود ممارسات وعمليات فعالة تتعلق بالبيئة الافتراضية سيضمن قدرة المؤسسة على تحسين القيمة الإجمالية لهذه التقنية.

شكل توضيحي (٩-٢)

الممارسات الجيدة لحوكمة تقنية المعلومات في البيئة الافتراضية

• **التأكـد من أن جميـع الأطراف المتأثرة تدرك مزايـا وعيوب البيئة الافتراضية:** قبـل انتقال تقنية المعلومـات من النظم الفعليـة القديمة إلى النظم الافتراضية، أو القيـام بإضافة مجموعة جديدة من الخـوادم الافتراضيـة لتنفيذ أعباء أعمال محددة، فإنه ينبغي عـلى إدارة تقنية المعلومات والإدارة أن يتأكدوا من فهمهم للقيود والحقائق المتعلقة بالبيئة الافتراضية من حيث استخدامات وحدة المعالجة المركزية والذاكرة ومجمل الضوابط الخاصة بحوكمة تقنية المعلومات.

• **تحديـد الأولويـات لإدارة النظم الافتراضية وتصحيحها وأمنها:** أي وضع قيود على عملية انتشـار الأجهزة الافتراضية، وتشـمل جميـع الأجهزة الافتراضية الموجودة في حزم تقنيـة المعلومات، والإدارة، والبنى التحتية الخاصة بسياسات الأمن.

• **التعامل مع النظم الافتراضية كما لو كانت نظماً فعلية في معظم الأحوال:** بشـكل عام فإنه يجب ألا تُعامل النظم الافتراضية كما لو كانت مختلفة عن أي من النظم الفعلية. لذا يجب أن يتم تطبيق النظـم الافتراضيـة وفقاً لمجموعة معرفة على نحو جيد من البيانات الخاصة بسياسـات وممارسـات الحوكمة والتي صُممت بالشكل الذي يضمن أن بيانات النظم الافتراضية:

o **يمكـن الوصول إليها:** بمعنى أنه يجب أن يتمكن مسـتخدمو النظـم الافتراضية من الوصول إلى البيانات التي يحتاجون إليها وبالصيغ التي تتوافق مع متطلباتهم.

o **آمنة:** تماماً كما هو الحال بالنسبة لجميع التطبيقات الاعتيادية، فقط الأشخاص المصرح لهم هم الذيـن يجب أن يُسـمح لهم بالوصول إلى بيانات النظم الافتراضية، أما الأشـخاص غير المصرح لهم بذلك فيجب أن يتم منعهم من الوصول إلى تلك البيانات.

o **متطابقة ومتناغمة:** عندما يقوم اثنان من المسـتخدمين بالبحث عن البيانات نفسـها، يجب أن يتم ترشيد "نفس" البيانات في إصدارات متعددة بصورة منتظمة.

o **عالية الجودة:** يجب أن تكون البيانات الصادرة عن تطبيقات البيئات الافتراضية دقيقة ومتطابقة لتلبية معايير تقنية المعلومات المعمول بها.

o **قابلة للتدقيق:** يجب أن يكون في البيئة الافتراضية مسـارات واضحة تشـير إلى مصادر البيانات، ورؤيـة واضحـة لأصل هذه البيانات، وضوابط تدل عـلى أن إدارة تقنية المعلومات تعلم من الذي يستخدم هذه البيانات وما الغرض من استخدامها؟

• **توظيف إجراءات نسخ احتياطي قوية للتطبيقات:** إن عمل نسخ احتياطية لكامل الجهاز الافتراضي يحتاج إلى وقت أكبر ويعطي القليل من الخيارات فيما يتعلق بعملية الاسترجاع السريع للنظم. ومع ذلك، فإنه يجب أن تقوم إدارة تقنية المعلومات بعمل نسـخ احتياطية وبشـكل منتظم من تطبيقات البيئة الافتراضية تماماً كما لو كان يقوم بحماية النظم الفعلية ذات المهام الحساسة، والتأكد من قدرة إدارة تقنية المعلومات على تنفيذ عمليات التعافي السريعة وزيادة الثقة بالتطبيقات كذلك.

• **التخزيـن المركزي للنظم:** السـبب الرئيـسي وراء زيادة الأجهزة الافتراضية غالباً هو انتشـار أجهزة الخوادم المضيفة الفعلية في جميع أنحاء المؤسسة. لذلك وفي ظل وجود النظم الافتراضية، فإن عملية نسـخ كامل لنظام الضيف (أو الاثنين) سـهلة جداً، وإن هذه السـهولة هي السبب الرئيسي في تزايد الأجهـزة الافتراضية وكذلك النتيجة المحتملة لفقدان البيانات. فإذا عجزت إدارة تقنية المعلومات عن تأمين الأجهزة الافتراضية التي لديها ، فلا بد أن يكون لديها أقراص مشفرة حقيقية أو افتراضية لضمان عـدم فقدان البيانات السرية. فعندما تقـوم بوضع أجهزة الخوادم المضيفـة الافتراضية الخاصة بك والوحدات التخزينية في أماكن مركزية آمنة، فإن إدارة تقنية المعلومات سـتتمكن من الحد من تزايد الأجهزة الافتراضية وكذلك احتمالية فقدان البيانات.

قضايا حوكمة الهواتف الذكية وأجهزة تقنية المعلومات المحمولة:

يستخدم الناس هذه الأيام وعلى اختلاف مستوياتهم أجهزة الهواتف الذكية والحاسبات اللوحية لممارسـة النشـاطات الشـخصية والمنزلية الخاصة بهم. وقد بدأ ذلك على شـكل هواتف خلوية شـخصية صغيرة وتطور الأمر على مر السـنين إلى أجهزة قادرة على الاتصال بالإنترنت، وإرسـال الرسائل النصية، والتقاط الصور وإرسـالها وما هو أكثر من ذلك بكثير. يمتلك الحاسب اللوحي Tablet الإمكانيات الموجودة في الحاسب الشخصي المحمول Laptop باسـتثناء لوحة المفاتيح الأكبر حجماً، فالحاسبات اللوحية أصغرُ حجماً، واخفُ وزناً، وقادرةٌ بالأساس على العمل كما لو كانت هواتف ذكية. وعلى الرغم من الميزات القوية والعديدة الموجودة في تلك الأجهزة، فإنها تعتبر نسبياً ذات تكلفة أقل. وقد أصبحت أجهزة شخصية تسـتخدم مـن قِبل العديد من العائلات ومن ضمنهم الأطفـال الصغار. وقد أشرنا في هذا القسـم إلى جميع هذه النظم باسـم الأجهزة المحمولة handheld devices، سـواء كانت هواتف ذكية، حاسبات لوحية، أجهزة تخزين صغيرة USB أم غيرها.

منذ عدة سـنوات ليسـت بالكثيرة لم تكن هذه الأجهزة المحمولة مسـتخدمة في أماكن العمل. إلا أن المؤسسـات قد قامت بتشـجيع الموظفين الرئيسـيين لديها باستخدام أجهزة الحاسـبات الشخصية المحمولة Laptop، وقامت بإصدار روابط آمنة لتمكنهم من الوصول إلى المنتجات البرمجية الخاصة بالمؤسسـة. فضلاً عن أن تلك الحاسبات الشخصية المحمولة Laptops كانت تعار للموظفين ليقوموا باستخدامها لأغراض العمل فقط، أما الاستخدامات الشـخصية لها فقـد كانت غير محبذة ولا ينصح بها، وكان الموظفـون يقومون بإعادة تلك الأجهزة إلى إدارة تقنية المعلومات بعد رحيلهم.

إن الاسـتخدام الشـخصي للموظفين للهواتف الذكية والأجهـزة اللوحية هذه الأيام قد يثـير بعض القضايا المتعلقـة بحوكمة تقنية المعلومات. فعلى سـبيل المثـال، تمتلك هذه الأجهزة عموماً ميزة الكاميرا الرقمية المدمجة فيها. وبالتأكيد يمكن أن يثير هذا الأمر مسألة أمنية على اعتبار أن الموظف يسـتطيع بسـهولة التقاط صور لوثائـق مهمة ومن ثم نقلها واسـتخدامها لأغراض غير مشروعة. فعلى الرغم من القوانين الصادرة والتي تمنع مثل تلك الممارسات، فإن المؤسسـة في الواقع لا تستطيع منع مثل تلك الممارسات المتعلقة بالتصوير الداخلي بالرغم من التصريحات السياسـية القوية ضد أنشطة كهذه. وكذلك الأمر بالنسبة لأجهزة التخزين الصغيرة USB المستخدمة من قبل العديد أيضاً، والتي يمكن توصيلها بأحد أجهزة الشركة لأخذ معلومات هامة وحساسة.

ترتبط العديد من المخاوف المتعلقة باستخدام الأجهزة المحمولة في أماكن العمل بالأمن المؤسسي. فالمؤسسة سـتكون مضطرة للسماح لأشخاص أساسيين للقيام بالاتصال بشبكات البيانات والتي تعد جزءاً من مسئوليات عملهم. فضلاً عن أن، هناك حاجة لتنصيب برامج الجدران النارية والبرامج المضادة للفيروسات والأدوات البرمجية لمراقبة الأمن على أي جهاز نقال سوف تُعطي له صلاحية الوصول للنظم الشبكية المؤسسية. ونظراً لكثرة أنواع الأجهزة الموجودة في المؤسسـة واختلاف أنواعها، فلن تستطيع المؤسسة ضبط عملية إصدار أجهزة كهذه، إلا أنها يجب أن تمتلك مجموعة من المعايير المثبتة واللازمة لضبط استخدام الأجهزة النقالة قبل السماح لها بالوصول إلى بيانات الشركة.

الشـــكل التوضيحي (٩-٣) يعد مثالاً على سياســـة الشركة فيما يتعلق باســـتخدام الأجهزة المحمولـــة من قبل الموظفين وأصحـــاب المصالح في بيئات العمل. يجـــب أن يتم إبلاغ جميع الموظفين الجدد بمثل هذه السياســـة إلى جانب مطالبتهم بقبولها بشكل رسمي. ولأن التقنية دائمـــة التغير، فمن الممكـــن أن تختلف اتجاهات وطبيعة الجهاز المحمول اليوم عما ســـتكون عليه غداً. لذلك فإن هذا النوع من بيان السياسة يجب أن يُعدل ويُعاد إصداره بشكل دوري ومنتظم مع ضرورة مطالبة المتلقين لتلك السياسة بالإفصاح عن فهمهم وقبولهم لتلك السياسة المنقحة. يجب أن تُستخدم العناصر الأساسية في هذه السياسة الخاصة بالأجهزة المحمولة من قبل الإدارة والتدقيق الداخلي على أنها جزء من مراجعاتهم المنتظمة للرقابة الداخلية.

شكل توضيحي (٩-٣)

سياسة استخدام الموظفين وغيرهم من أصحاب المصالح للأجهزة المحمولة

مقدمة: إن اســـتخدام الأجهزة المحمولة في بيئات عمل شركتنا في ازدياد، وهي تقدم خدمات الأجهزة النقالة والاتصال المســـتمر بالأجهزة النقالة للعاملين. ونظراً لحقيقة أن الأجهزة المحمولة تكون غالباً ممتلكات شخصية لأصحابها. فهي تشكل تهديدات جديدة لأصول الشركة. وتشمل الأجهزة المحمولة التي تحمل تحدياتٍ أمنية كلاً من الحاســـبات الشـــخصية المحمولة ووحدات التخزين المتحركة (مثل جهاز USB) والهواتف الذكية والحاسبات اللوحية وغيرها من الكاميرات.

الغرض والنطاق: تضع هذه السياســـة الأمنية قواعد تتعلق بالاســـتخدام الصحيح للأجهزة المحمولة في جميـــع أنحـــاء الشركة، وذلك من أجل حماية سرية البيانات الحساســـة، وســـلامة كل من البيانات والتطبيقـــات، وإتاحة خدمات شركتنا. إن هذا من شـــأنه أن يحمي الأجهزة المحمولة ومســـتخدميها بالإضافة إلى أصول الشركة (سريتها وسلامتها) واستمرارية الأعمال (إتاحتها).

وتُطبق هذه السياسة على جميع الموظفين، والاستشاريين، والموردين، والمقاولين والطلاب وغيرهم ممن يستخدمون الأجهزة المحمولة النقالة الخاصة أو المرتبطة بالأعمال داخل أي مبنى من مباني شركتنا.

إن الالتزام بهذه المتطلبات وبالسياســـات الأمنية المنبثقة منها والأحكام التنفيذية يعد أمراً ملزماً في جميع أنحـــاء شركتنا وفروعها وغالبية ممتلكاتها. و يعتبر التعدي المقصود على هذه السياســـات أو الإهمال فيها تهديداً لمصالح شركتنا وسيؤدي إلى عقوبات صارمة وظيفية كانت أو قانونية أو كليهما معاً. وستطبق أيضاً هذه الشروط والسياسات الأمنية المنبثقة منها والأحكام التنفيذية على جميع الموردين التابعين لشركتنا.

الأدوار والمســؤوليات: إن جميــع الموظفين وأصحاب المصالح مســؤولون عن التقيــد بهذه الأحكام الأمنية. وقد تم توثيق المهام المحددة عند تعريف الأدوار، ويجب تحديد شخص بالاسم لكل دور من هذه الأدوار وأن يكون معروفاً بالنسبة لإدارة أمن تقنية المعلومات.

المسؤوليات المتعلقة بحوكمة تقنية المعلومات:

• أصحاب وحدات الأعمال: ضمان تزويد إدارة تقنية المعلومات بالمصادر الضرورية.

• إدارة تقنية المعلومات: المحافظة على السياسات الأمنية:

- مسؤولة عن إيجاد سياسات أو تبني السياسات المعمول بها وصيانتها لمواكبة العصر.

- تُطبق التوجيهات والإجراءات اللازمة لتنفيذ هذه السياسة وتقوم بتبليغها للأشخاص المعنيين.

- تَضمن أن جميع الإجراءات القابلة للتطبيق موثقة وتم إيصالها بشكلٍ جيدٍ.

- مسؤولة عن فرض السياسة وضمان أن المستخدمين قد تلقوا التدريبات الملائمة.

• إدارة أمن تقنية المعلومات: مسئولة عن إدارة جميع الأجهزة المحمولة النقالة التي يتم إصدارها:

- تقوم بإدارة مستودع الأجهزة المحمولة المسجلة.

- تضمن أن الخدمات الضرورية متاحة للمستخدمين وتقوم بتقديم الموارد الضرورية لاستخدام تلك الخدمات.

- مسؤولة عن فرض السياسة:

o من خلال ضوابط العمل المناسبة.

o تقديم طلبات تتعلق بالتغيرات الضرورية في هذه السياسة لدعم حوكمة تقنية المعلومات.

• **المستخدمون وغيرهم من أصحاب المصالح:** يجب على موظفي المؤسسة وأصحاب المصالح أن يقوموا بقراءة هذه السياسات الأمنية وفهمها والموافقة عليها، ويجب عليهم أيضاً إعلام إدارة تقنية المعلومات بالمخالفين لهذه السياسات الأمنية.

ملاحظة:

1. SAS 70, “Service Auditors Reports,” http://sas70.com/sas70_reports.html

الفصل العاشر

الحوكمة وإدارة أمن تقنية المعلومات وإدارة الاستمرارية

تعد العمليات الفعالة والخاصة بإدارة أمن تقنية المعلومات واستمراريتها من العناصر الهامة للحوكمة الشاملة لتقنية المعلومات المؤسسية. إن أمن تقنية المعلومات مصطلح واسع، فهو يشير إلى العمليات والضوابط اللازمة لحماية كل من النظم والبيانات الخاصة بتقنية المعلومات بالإضافة إلى الأصول المادية في المؤسسة من مجموعة واسعة من التهديدات المحتملة. ففي عالمنا اليوم القائم على الإنترنت، إضافة إلى المخاطر القادمة من أشخاص من جميع أنحاء العالم ربما يكونو مُولَعِين بالوصول غير المشروع للأنظمة المؤمنة، أصبحت قضية أمن تقنية المعلومات الآن تحظى بالاهتمام بل وتزايد الاهتمام بها أكثر من أي وقت مضى. لذا فإن المؤسسات تحتاج إلى تطبيق عمليات فعالة خاصة بأمن تقنية المعلومات للتحكم في أصول تقنية المعلومات الخاصة بها وضبطها.

وعلى الرغم من أهمية عمليات الأمن الموضوعة لحماية الأصول الخاصة بتقنية المعلومات من الأشخاص غير المصرح لهم، فإن عمليات التشغيل الخاصة بتقنية المعلومات أيضاً تواجه تهديدات من مخاطر مثل: اندلاع حريق في أحد المرافق، أو كوارث طبيعية، أو أعطال المعدات. وقد كان يعرف هذا المجال الخاص بالمخاوف المتعلقة بمخاطر تقنية المعلومات بالتخطيط للتعافي من كوارث تقنية المعلومات IT disaster recovery planning وذلك في الأيام الأولى لظهور تقنية المعلومات عندما كانت نظم الحاسبات المركزية maiframe هي المهيمنة، أما اليوم فهي بشكل عام تسمى تخطيط استمرارية تقنية المعلومات IT continuity planning. لذا يجب على المؤسسة امتلاك الموارد اللازمة لعمل النسخ الاحتياطية، سواء كانت لمعدات أم لبرمجيات، وذلك لاستمرار العمليات التشغيلية المنتظمة والمجدولة في حال حدث أي انقطاع غير طبيعي لها.

يناقش هذا الفصل السؤال التالي: لماذا يعد وجود عمليات معمول بها لأمن واستمرارية تقنية المعلومات أمراً في غاية الأهمية بالنسبة للحوكمة الفعالة لتقنية المعلومات؟ تكون العمليات الفعالة لتخطيط أمن واستمرارية تقنية المعلومات معقدة غالباً وتحتاج إلى

مهـارات المتخصصـين. لذا يجب على المدير الأول الذي يعمل عـلى توجيه ومراجعة حالة جميع عمليات حوكمة تقنية المعلومات أن يتمتع بقدر معين من المعرفة الأساسية نوعاً ما لبعض الأدوات والإجراءات الفعالة المستخدمة في هذا المجال. ومع أن كلاً من هذه الأدوات والإجـراءات يعتبر من المجالات المتخصصة، فإنها أيضاً تعتبر من العناصر الهامة والضرورية للحوكمة الشاملة الفعالة لتقنية المعلومات في المؤسسة.

أهمية البيئة الفعالة لأمن تقنية المعلومات:

لقـد تغير مفهوم أمن تقنية المعلومات كثيراً على مر السـنين وأصبـح أمراً أكثر تعقيداً. فبالعودة إلى عصر نظم الحاسـبات المركزية، كنا نعتقد أن أمن تقنية المعلومات لا يتعدى أنظمة بسـيطة لكلمة المرور ووضع أقفال على أبواب مركز الحاسـب. وقد كان من المهم في ذلـك الوقت أن تكون أصول تلك النظم محمية ويتم عمل نسـخ احتياطية لها بشـكل متكـرر. وكانت تقع مسـئولية تلك العمليات على عاتق وحدة أو إدارة عمليات تشـغيل تقنية المعلومات مع تدخل محدود من قبل الإدارة العامة.

أمـا في هذه الأيام، وفي ظل تكرار النشرات الإخبارية حول تلك الأحداث المتعلقة بتقنية المعلومات كسرقة ملفات النظم الحاسـوبية الخاصة بالبطاقات الائتمانية، أو إفشاء ما هو مـن المفترض أن يكون ملفات لرسـائل سرية خاصة بنظام الحاسـب، أصبحت قضايا أمن تقنية المعلومات مسـألة هامة بالنسـبة للعديد من أعضاء فريق تقنية المعلومات والإدارة العامة للمؤسسـة. وعلى الرغم من أن قضية أمن تقنية المعلومات كانت دائماً ومنذ الأيام الأولى مصـدر قلـق، فإن مجال المخاطر هذا أصبح مصدر قلـق أكثر من ذلك بكثير في عالم اليوم الذي يحوي كماً هائلاً من اتصالات الإنترنت وكذلك الاعتماد المتزايد على إستراتيجيات الحوسبة السحابية. يكون التدقيق الداخلي والإدارة العليا في المؤسسات غالباً هم الأطراف المعنيـة بالقراءة عن الخروقات الخاصة بأمن تقنيـة المعلومات التي تحدث في مكان آخر وسـؤال كل من المدير التنفيذي للمعلومات (Chief Information Officer (CIO ومدير التدقيـق الداخـلي (Chief Audit Executive (CAE ومدققـي تقنيـة المعلومات حول المسائل المتعلقة بأمن تقنية المعلومات في المؤسسة.

تعـد المخاوف المتعلقة بأمـن تقنية المعلومات من بين القضايا الرئيسـية والهامة التي تؤثـر في كل مـن الإدارة العامـة وإدارة تقنية المعلومات. وللحصـول على ضمانات كافية حول امتلاك أمن فعال لتقنية المعلومات، فإن المؤسسة بحاجة إلى تأسيس وبناء بيئة قوية ومـدارة بشـكل جيد لأمن تقنية المعلومـات. وتعد هذه المهمة مسـئولية إدارة عمليات تشـغيل تقنية المعلومات وإدارة المؤسسة على جميع المستويات. فإدارة تقنية المعلومات تسـتطيع المسـاعدة في هذه العملية من خـلال تطبيق ضوابط داخلية فعالة وسياسـات وإجراءات أمنية قوية، وكذلك من خلال العمل مع جميع المسـتويات في المؤسسـة لخلق بيئة أمنية فعالة.

سـوف يركز هذا الفصل على بناء بيئة فعالة لحوكمـة أمن تقنية المعلومات وذلك من ثلاثـة منظـورات: المنظور الأول، هو أن هناك حاجة لوضع بعـض المبادئ القوية الخاصة بأمـن نظم تقنية المعلومات، مثل المبادئ التي تمت مناقشـتها في الفصل الخامس من هذا الكتـاب والذي يدور حول الكوبت، أو تطبيق معايير الأيزو المناسـبة التي تناولنا الحديث عنها في الفصل السـابع أيضاً من هذا الكتاب. إذ يمكن أن تلعب هذه المبادئ دوراً أساسياً في المساعدة على تأسيس بيئة فعالة لأمن تقنية المعلومات.

أمـا في ما يخص المنظور الثاني، فهناك حاجة ماسـة لتأسـيس أمن فعـال لمحيط تقنية المعلومـات، وذلك في أي عملية تقريباً من عمليات التشـغيل الخاصـة بتقنية المعلومات. فعلى الرغم من أن المخاطر التي كانت تواجه عمليات تشـغيل الحاسب التي كانت تتم في مركز مغلق أيام الحاسـبات المركزية أقل بكثير من المخاطر التي تواجه عمليات التشـغيل اليـوم، فإن المخاطر الأمنية تعد أكبر بكثير في البيئات الخاصة بالتجارة الإلكترونية المعتمدة على شبكة الإنترنت. وسنتحدث عن بعض الضوابط الأمنية الخاصة بمحيط تقنية المعلومات التي ينبغي أن تسهم في التحسين من عمليات حوكمة تقنية المعلومات في تلك المجالات.

أما بالنسبة للمنظور الثالث، فسـوف نناقش من خلاله أهمية وضع إستراتيجية أمنية فعالة على مسـتوى المؤسسـة. تمامـاً مثل مدونة قواعد السـلوك للموظـف التي تضع مجموعة من القواعد الرفيعة المستوى لجميع أصحاب المصلحة في المؤسسة. فالإستراتيجية الفعالة لأمن تقنية المعلومات هي التي تقوم بتأسـيس بعض القواعد المتعلقة بأمن تقنية

المعلومات. إذ يمكن للإستراتيجية الأمنية لتقنية المعلومات المُصممة والمُطبقة على نحو جيد أن تسهم في تحسين العديد من الجوانب الخاصة بعمليات التشغيل في المؤسسة. كما ينبغي على إدارة تقنية المعلومات أن تكون على دراية بأفضل أو أجود الممارسات الفعالة في هذا المجال، وأن تقوم باستخدام تلك الممارسات لتأسيس بيئة فعالة لأمن تقنية المعلومات.

مبادئ أمن تقنية المعلومات في المؤسسة: المعايير الأمنية المتفق عليها:

إن العديد من كبار المديرين اليوم على علم بما يعرف بالمبادئ المحاسبية المقبولة قبولاً عاماً General Accepted Accounting Principles (GAAP) سواء كان ذلك من خلال أعمالهم الخاصة أو اتصالاتهم مع المديرين الماليين في المؤسسة أو مع مدققيهم الخارجيين. وعلى الرغم من أنه استُبْدِل اليومَ بتلك المبادئ (GAAP) بمعاييرَ محاسبية دولية، فإنها تعد بمثابة قواعد غير رسمية تستخدم من قبل العديد من المديرين الماليين ومدققيهم الخارجيين لتقييم الممارسات المحاسبية في المؤسسة، ومن ثم القيام بإعداد القوائم المالية الخاصة بها. فهي ليست قواعد محددة على شكل نقاط، إنما هي عبارة عن مجموعة من الممارسات الجيدة والعامة التي استُخدمت من قبل المدققين الخارجيين على مر السنين.

بأسلوب مماثل للمبادئ المحاسبية المقبولة قبولاً عاماً GAAP، قامت العديد من إدارات تقنية المعلومات المؤسسية بتطبيق ما يعرف بمبادئ أمن النظم المقبولة قبولاً عاماً Generally Accepted System Security Principles (GASSP) كمجموعة من أفضل الممارسات لتطوير عمليات ومعايير فعالة في أمن تقنية المعلومات. GASSP هي عبارة عن مجموعة متفق عليها من المبادئ والمعايير والأعراف والآليات المتعلقة بأمن تقنية المعلومات التي يجب أن توظف من قبل الممارسين لقضايا أمن تقنية المعلومات، والتي يجب أن تحققها المخرجات الناتجة عن معالجة المعلومات، والتي يجب أن يقر بها أصحاب المعلومات لضمان أمن المعلومات وأمن نظم تقنية المعلومات الخاصة بهم. تتعلق GASSP بأمن المعلومات المادية والتقنية والإدارية، كما تشتمل على مبادئ أمنية تفصيلية ووظيفية واسعة ومتعارف عليها. تشير GASSP إلى سلسلة من القواعد والإجراءات والممارسات التي تتعلق بتطبيق الممارسات الفعالة لأمن تقنية المعلومات في المؤسسة. ومن المتوقع

أن يتطــور هذا المفهوم الخــاص بمصطلح GASSP وفقاً للتغيرات السريعة والمســتمرة في التقنيات الخاصة بتقنية المعلومات.

تعــود أصول هذه المبادئ المقبولة قبولاً عاماً في أمن معلومات النظم GASSP إلى عام ١٩٩٠ عندما قام مجلس البحوث الوطني الأمريكي بإصدار كتاب أحدث تحولاً بارزاً بعنوان "الحاســبات عرضة للمخاطر"[١] Computers at Risk (CAR)، وقد ركز هذا الكتاب على أن الولايات المتحدة الأمريكية بحاجة ماســة إلى أن تركز اهتمامها بشــكل أفضل على أمن المعلومــات. وقد وُجدت GASSP لتكون نتيجة مباشرة لإحدى التوصيات الرئيســية التي جاءت من نشر هذا الكتاب (CAR) وقد دعت تلك التوصية إلى تطوير مجموعة شاملة من المبادئ المقبولة قبولاً عاماً في أمن النظم والتي من شــأنها أن تقدم تعريفاً واضحاً للسمات والضمانات والممارســات الأساســية الخاصة بأمن تقنية المعلومات. كما اقترح كتاب CAR استخدام GAAP نموذجاً يُقتدى به في وضع GASSP، كما استشهد أيضاً بالصياغة الخاصة بالقواعــد والمعايير المســتخدمة من قبل مختــبرات ضمان المواصفــات[٢] Underwriters Laboratories بأنها أمثلة على GASSP في مجالات أخرى.

يعد الاتحــاد الدولي لاعتماد أمن نظــم المعلومــات[٢] International Information Systems Security Certification Consortium (ISC) مــن المنظمات المهنية الأخرى الرائدة في أمن تقنية المعلومات والتي قامت بتطوير GASSP في نســخته الحالية (الإصدار الثاني Version 2.0) والتي تم إطلاقها في عام ١٩٩٣[٣]. وكما يدل عليها اسمها، فهي عبارة عن المبادئ المقبولة قبولاً عاماً أو المتعارف عليها، الأمر الذي يعني أنها تَســتخدم المفاهيم الشائعة الاستخدام في وقتنا الحاضر لتأمين موارد تقنية المعلومات. إن المبادئ التي جاءت في الدراسة الخاصة بمفهوم GASSP ليست جديدة بالنسبة للعاملين في أمن تقنية المعلومات، ولكنهــا اعتمدت على افتراضات ينبغي تقريباً على كل شــخص تطبيقها عند القيام بتطوير أو صيانة نظام أمن تقنية المعلومات. لذا يجب على مدير المؤسســة التي تسعى إلى تعزيز العمليــات الأمنية لتكون جزءاً من الحوكمة الفعالة لتقنية المعلومات، أن يكون على دراية بمبادئ GASSP بوصفة معياراً أو أسلوباً لتعزيز الأمن الفعال لتقنية المعلومات.

المبادئ المتعارف عليها في أمن النظم والمقبولة عموماً GASSP:

ترتكـز GASSP على ثمانية مبادئ رفيعة المسـتوى يمكن أن تسـتخدم من قِبل الإدارة وأخصائيـي أمن تقنية المعلومات أساسـاً أو قاعدة ليقوموا ببنـاء برامجهم المتعلقة بأمن تقنية المعلومات عليها. وتهدف هذه المبادئ لأن تكون بمثابة دليل أمني يمكن اسـتخدامه عند إنشـاء نظم أو ممارسـات أو سياسات جديدة. فهي لم تُصمم لإعطاء إجابات محددة، بل يجب تطبيقها جملة واحدة وبشـكل عملي ومعقول. وفيما يلي توضيح لكل من هذه المبادئ الثمانية الخاصة بمفهوم GASSP.

١. **يجـب على أمن تقنية المعلومات دعم رسـالة المؤسسـة:** إن الغـرض من أمن تقنية المعلومـات هو حماية الموارد القيّمة في المؤسسـة كالمعلومات والمعـدات والبرمجيات. فمن خلال اختيار وتطبيق وسـائل الحماية المناسـبة، يمكن للأمن أن يسـاعد المؤسسة على تحقيق رسـالتها، وذلك من خلال حماية مواردها المادية والمالية وسمعتها ووضعها القانوني وموظفيها وغيرها من الأصول الملموسـة وغير الملموسـة. وللأسـف فإنه يُنظر لأمن تقنية المعلومات في بعض الأحيان على أنه عائق في طريق تحقيق رسـالة المؤسسة، وذلك من خلال فرض القواعد والإجراءات المُرْهِقَة التي يتم اختيارها بشـكل سيئ، على المستخدمين والمديرين والنظم. ونتيجة لذلك فإنه يجب على إدارة تقنية المعلومات أن تكون على علم بأن القواعد والإجراءات الأمنية التي تم اختيارها بعناية لم تُوضع لحماية مصالحهـم الخاصـة، وإنما وضعت موضع التنفيذ لحماية الأصول الهامة ودعم الرسـالة التنظيمية الشاملة للمؤسسة.

ولذلك فالأمن يعد وسيلة للوصول إلى الغاية وليس غاية في حد ذاته. فعلى سبيل المثال، يكون للممارسات أو الإجراءات الأمنية المستخدمة عادةً دور ثانوي في عملية تحقيق الأرباح المؤسسية التي هي الهدف الرئيسي لأي مؤسسة. لكن يجب بعد ذلك أن يكون للأمن دور رئيسي في زيادة قدرة المؤسسة على تحقيق الأرباح. أما في مؤسسات القطاع العام، فيلعب الأمن عـادة دوراً ثانوياً فيما يتعلـق بالخدمات التي تقدمها المؤسسـة للمواطنين، إلا أنه يتوجب على الأمن فيما بعد أن يلعب دوراً أساسياً في تحسين هذه الخدمات العامة. لذلك فإن المديرين وأخصائيي الأمن بحاجة إلى فهم كلٍّ من الرسـالة الشاملة للمؤسسة والكيفية

التي يمكن من خلالها أن يقوم كل نظام من نظم تقنية المعلومات بدعم تلك الرسالة. وبعد أن يتـم تحديد أدوار تلك النظم، يمكن الإعـلان صراحة عن تلك المتطلبات الأمنية الخاصة برسالة المؤسسة.

٢. **أمن تقنية المعلومات جزءٌ لا يتجزأ من الممارسات الإدارية الصحيحة:** تكون نظم تقنية المعلومات غالباً من الأصول الهامة التي تدعم رسالة المؤسسة. لذا فحماية تلك الأصول أمر لا يقل أهمية عن حماية الموارد الأخرى، مثل الأموال أو الأصول المادية أو الموظفين. مـن ناحية أخـرى، فإن تضمين الاعتبارات الأمنية في إدارة نظـم المعلومات وإدارة نظم تقنية المعلومات لا يسـتبعد بشـكل كامـل احتمالية أن يتـم الإضرار بهذه الأصول. في النهاية، يجب على الإدارة أن تقرر ما مسـتوى المخاطر المسـتعدة لقبولها، مع الأخذ في الحسبان تكلفة الضوابط الأمنية.

كما هو الحال مع غيرها من الموارد، فإن إدارة نظم المعلومات وإدارة نظم تقنية المعلومات قد تتجاوز الحدود التنظيمية. فعندما تكون نظم معلومات ونظم تقنية المعلومات الخاصة بالمؤسسة مرتبطة بنظم خارجية، فإن مسؤوليات الإدارة ستمتد لتتجاوز حدود المؤسسة، وإن كلاً من الإدارة وإدارة تدقيق تقنية المعلومات يجب أن يعرفوا ما مسـتويات أو أنواع الأمن التي يتم توظيفها على تلك النظم الخارجية، كما يجب أن يسعوا للحصول على ضمانات بأن النظام الخارجي يوفر الأمن الكافي لاحتياجات المؤسسة التابعين لها.

٣. **أمـن تقنيـة المعلومات يجـب أن يكون فعالاً من حيث التكلفـة:** يعد هذا الأمر من المبـادئ الهامة لحوكمـة تقنية المعلومـات. وعليه فإنه يجب عمل دراسـة للتكاليف والفوائد الخاصة بأمن تقنية المعلومات بعناية، سـواء مـن الناحية المالية أم غير المالية للتأكـد من أن تكلفـة الضوابط لن تزيد عن الفوائد المتوقعـة. فأمن تقنية المعلومات يجـب أن يكون ملائماً ومتناسـباً مع قيمة ودرجة الاعتماد على نظـم تقنية المعلومات وكذلـك مع شـدة واحتمالية ومدى الـضرر المحتمل. كما أن المتطلبـات الأمنية تتنوع اعتماداً على النظام المحدد لتقنية المعلومات.

يجـب أن يُنظر لأمن تقنية المعلومـات على أنه أحد الممارسـات الذكية للأعمال. وأن الاسـتثمار الجيد في التدابير الأمنية للمؤسسـة يمكن أن يساعد في التقليل من تكرار وشدة

الخسـائر المتعلقة بأمن تقنية المعلومات. فعلى سـبيل المثال، قد تقدر المؤسسة أنها تعاني من خسـائر سنوية كبيرة في المخزون من خلال المعاملات الاحتيالية التي تتم في نظام تقنية المعلومات الخاص بمراقبة المخزون لديها. فباسـتخدام التدابير والإجراءات الأمنية المناسبة، كالنظام المطور الخاص بضبط عمليات الوصول للبيانات، قد يسـهم بشكل كبير في التقليل مـن هذه الخسـائر. علاوة على ذلك، فإن البرنامج الأمني السـليم يمكنه إحباط محاولات القراصنة Hackers والتقليل من تكرار الإصابة بالفيروسات.

للفوائد الأمنية تكاليف مباشرة وغير مباشرة. حيث تشتمل التكاليف المباشرة على شراء وتركيـب وإدارة التدابـير والإجراءات الأمنية، كبرامج ضبط الوصـول إلى البيانات أو النظم المسـتخدمة لإخماد الحرائق في مرافق المؤسسـة. هذا بالإضافة إلى أن اسـتخدام التدابير والإجـراءات الأمنية قد يؤثر في بعض الأحيـان في أداء النظم وفي معنويات الموظفين وحتى في المتطلبـات الخاصـة بإعادة التدريـب. فكل هذه الأمور يجـب أن تُؤخذ بعين الاعتبار بالإضافة إلى التكلفة الأساسـية الخاصة بالضوابط الأمنية لتقنية المعلومات نفسها. في كثير مـن الحالات، كما هو الحال بالنسـبة لتكاليف إدارة حزمة ضبـط الوصول للبيانات، يمكن لهـذه التكاليف الإضافية أن تتجـاوز التكاليف المبدئية المخصصـة للضوابط الأمنية. لذا يجـب عـدم اختيار الحلول الأمنيـة إذا كانت تكلفتها من الناحية الماليـة أو غير المالية أو المباشرة أو غير المباشرة ببساطة أكبر من تكلفة تحمل المشكلة.

٤. **لدى أصحاب النظم مسـؤوليات أمنية خارج مؤسساتهم:** إذا كان للنظام مستخدمون من خارج المؤسسـة، فإنه يقع على عاتق أصحاب هذا النظام مسـؤولية مشاركة هؤلاء المستخدمين بالمعلومات المناسبة والضرورية المتعلقة بالتدابير الأمنية المستخدمة ومدى النطاق العام لها، الأمر الذي يزيد مسـتوى الثقة لدى هؤلاء المسـتخدمين بأن نظامهم آمن بشكل كافٍ. ولا يعني هذا أنه يجب على جميع النظم تحقيق المستوى الأدنى من أمن المعلومات، وإنما يعني أنه يجب على أصحاب النظم إبلاغ عملائهم أو مستخدميهم بطبيعة وآلية أمن المعلومات المستخدمة لديهم.

إن الاختلاف بين المسـؤولية والمساءلة المتعلقة بأمن تقنية المعلومات ليس واضحاً دائماً. بشكل عام نستطيع القول إن "المسؤولية" هي مصطلح أوسع يحدد الواجبات والسلوكيات

المتوقعة. إذ يدل مصطلح المسـؤولية على الموقف الاسـتباقي من جانب الطرف المسؤول، وعلى العلاقة السببية بين الطرف المسؤول ونتيجة محددة. في حين يشير مصطلح "المساءلة" بشكل عام إلى قدرة تحمل الأشخاص لمسؤولية أفعالهم. لذلك قد يكون الأشخاص مسؤولين عن أفعالهم دون أن يتعرضوا للمحاسبة القانونية عنها. على سبيل المثال، المستخدم المجهول الهوية الذي يقوم باسـتخدام أحد النظم يكون مسـئولاً أن يتصرف وفقاً للمعايير المقبولة والمتفـق عليها، إلا أنه لا يُمكن مسـاءلته إذا قام بأي انتهـاك للبيانات أو النظم، إذ لا يمكن تتبع العمل المتسبب في الانتهاك الأمني الذي يقوم به شخص ما.

يدل هذا المفهوم ضمنياً على أن الناس والمؤسسات يتشاركون في المسؤوليات والمساءلات المتعلقـة بنظم تقنية المعلومات الخاصة بهم. فبالإضافة إلى مشـاركة المعلومات المتعلقة بالأمـن، يجب على مديري المؤسسـات أن يتصرفوا في الوقت المناسـب ويتخـذوا الإجراء المناسـب لمنع الخروقات الأمنية والرد عليها لمساعدة الآخرين وحمايتهم من الضرر. فضلاً عن أن اتخاذ مثل هذا الإجراء يجب ألا يُعرض أمن النظم للخطر.

٥. **المسـؤوليات والمسـاءلات الخاصة بأمن تقنية المعلومات يجب أن تتم بشكل صريح:** يجب أن تكون المسـؤوليات والمسـاءلات الأمنية واضحة وصريحة، سـواء أكانت تخص أصحاب ومقدمي ومسـتخدمي نظـم تقنية المعلومات أم غيرهم مـن الأطراف المعنية بأمن نظم تقنية المعلومات. وقد يكون نطاق هذه المسؤوليات داخل المؤسسة أو خارج حدودها. حتى وإن كانت مؤسسة صغيرة فإنه يجب أن تقوم بإعداد الوثائق التي تحدد السياسات الأمنية والمسئوليات الواضحة لأمن تقنية المعلومات للمؤسسة. على كل حال، فلا يُقصد بهذا المفهوم وجوب مسـاءلات الفرد عن جميع النظم. فعلى سبيل المثال، لا تَسأل العديد من نظم نشر المعلومات عن هوية المستخدم ولا تستخدم أياً من الوسائل التقنية الأخرى لتحديد هويته، ومن ثم لا يمكنها مساءلة المستخدمين.

٦. **أمـن تقنيـة المعلومات يتطلب نهجاً شـاملاً ومتكامـلاً:** إن توفير أمـن فعال لتقنية المعلومـات يتطلب اسـتخدام نهج شـامل يأخذ بعـين الاعتبار مجموعـة متنوعة من المجـالات الموجودة داخل وخارج مجال أمن تقنيـة المعلومات، وتمتد طوال دورة حياة نظـم المعلومات بالكامل. ولكي تعمل الضوابـط الأمنية بفاعلية، فإنها تعتمد غالباً على

التوظيف السليم للضوابط الأخرى، إذ هناك العديد من الاعتمادات المتبادلة فيما بينها. فإذا تم اختيار الضوابط الإدارية والتشغيلية والتقنية بشكل سليم فيمكنها أن تعمل معاً بصورة تعاونية. من ناحية أخرى، فإن عدم فهم المؤسسة للاعتمادات المتبادلة للضوابط الأمنية، قد يُضعف بعضها بعضاً. فعلى سبيل المثال، عدم تلقي التدريب المناسب المتعلق بطريقة وزمن استخدام حزم برامج الكشف عن الفيروسات قد يجعل المستخدمين يطبقون هذه الحزم بشكل خاطئ، ومن ثم يُصبح استخدام تلك الحزم غير فعال. ونتيجة لذلك قد يعتقد المستخدمون خطأً أنه إذا تم فحص النظام لمره واحدة فقط، فإنه سيكون دائماً خالياً من الفيروسات، ونتيجةً لذلك الاعتقاد الخاطئ ربما تنتشر الفيروسات بشكل غير مقصود. في الواقع، تكون تلك الاعتمادات المتبادلة أكثر تعقيداً ومن الصعب جداً التحقق منها.

تعتمد فاعلية الضوابط الأمنية أيضاً على عوامل مثل إدارة النظم، والقضايا القانونية، وضمان الجودة، والضوابط الداخلية والإدارية. كما يحتاج أمن تقنية المعلومات أيضاً إلى العمل مع الإدارات الأمنية التقليدية في المؤسسة متضمنة وحدات أمن الممتلكات والأفراد. كما يوجد العديد من الاعتمادات المتبادلة الأخرى الهامة التي تكون عادة فريدة بالنسبة لبيئة المؤسسة أو بيئة النظام. لذا يجب على المديرين أن يدركوا كيف يرتبط أمن تقنية المعلومات مع المجالات الأخرى للنظم وكيف يرتبط أيضاً مع إدارة المؤسسة.

٧. **يجب إعادة تقييم أمن تقنية المعلومات بشكل دوري:** تمتاز نظم تقنية المعلومات والبيئات التي تعمل فيها بأنها متغيرة. أي أن تقنية ومستخدمي النظام، والبيانات والمعلومات داخل النظام، والمخاطر المرتبطة بالنظام، والمتطلبات الأمنية جميعها دائمة التغير. وهناك عدة أنواع من التغيرات التي يمكن أن تؤثر في أمن النظم، تشمل التطورات التقنية، والتغيرات في قيمة أو استخدام المعلومات، وظهور تهديدات جديدة. أضف إلى ذلك، أنه لم يتم اختبار الأمن ولم يكن مكتملاً عند تطبيق النظام. ويتمكن مستخدمو ومشغلو النظام غالباً من اكتشاف أساليب جديدة لتجاوز أو تقويض الأمن، سواء كان ذلك بقصد أم بدون قصد. فالتغيرات التي تطرأ على أحد نظم تقنية المعلومات أو البيئة

التشغيلية الخاصة به يمكن أن تتسبب في إيجاد ثغرات أمنية جديدة. كما أن الالتزام والتقيد الصارم بالإجراءات الأمنية أمرٌ نادر جداً، بل إن هذه الإجراءات تصبح قديمة بمرور الوقت، الأمر الذي يجعل من الضروري إعادة تقييم أمن نظم تقنية المعلومات بشكل دوري.

٨. **أمن تقنية المعلومات مُقيد بعوامل اجتماعية:** قد تكون قدرة أمن تقنية المعلومات على دعم رسالة المؤسسة محدودة ومقيدة بعوامل مثل القضايا الاجتماعية، فقد يحدث تعارض بين الأمن وخصوصية مكان العمل. فعلى سبيل المثال، يتم تطبيق أمن نظم تقنية المعلومات غالباً من خلال تحديد المستخدمين ومتابعة أعمالهم التي يقومون بها. من ناحية أخرى، تتنوع توقعات الخصوصية كما يمكن أن يتم انتهاكها من خلال بعض التدابير الأمنية. ومع أن الخصوصية تعد قضية اجتماعية في غاية الأهمية، فإنها ليست المسألة الوحيدة المهمة. فتدفق المعلومات، وخاصة بين الحكومة ومواطنيها، تعتبر حالة أخرى قد تحتاج الإجراءات الأمنية فيها إلى بعض التعديلات لدعم الهدف المجتمعي. هذا بالإضافة إلى أن بعض التدابير المستخدمة للتحقق من صلاحيات مستخدمي النظم يمكن اعتبارها اختراقات للخصوصية في بعض البيئات والثقافات.

لذلك يجب أن يتم تحديد الإجراءات الأمنية وتنفيذها في ظل الاعتراف بحقوق الآخرين ومصالحهم المشروعة. وقد يتطلب ذلك تحقيق مزيد من التوازن بين الاحتياجات الأمنية لأصحاب المعلومات والمستخدمين وبين الأهداف المجتمعية. فضلاً عن أن القواعد والتوقعات تتغير إزاء الاستخدام الملائم للضوابط الأمنية. وهذه التغيرات إما أن تزيد أو تقلل من الأمن. وليس بالضرورة أن تكون العلاقة بين المعايير الأمنية والمجتمعية علاقة عدائية. فالأمن يستطيع أن يعزز الوصول إلى البيانات والمعلومات وتدفقها من خلال توفير معلومات أكثر دقة وموثوقية وإتاحة أكبر للنظم. كما يستطيع الأمن أيضاً زيادة الخصوصية الممنوحة للفرد أو المساعدة على تحقيق أهداف مجتمعية أخرى تم وضعها من قبل المجتمع.

تطبيق المبادئ الأمنية في إدارة تقنية المعلومات:

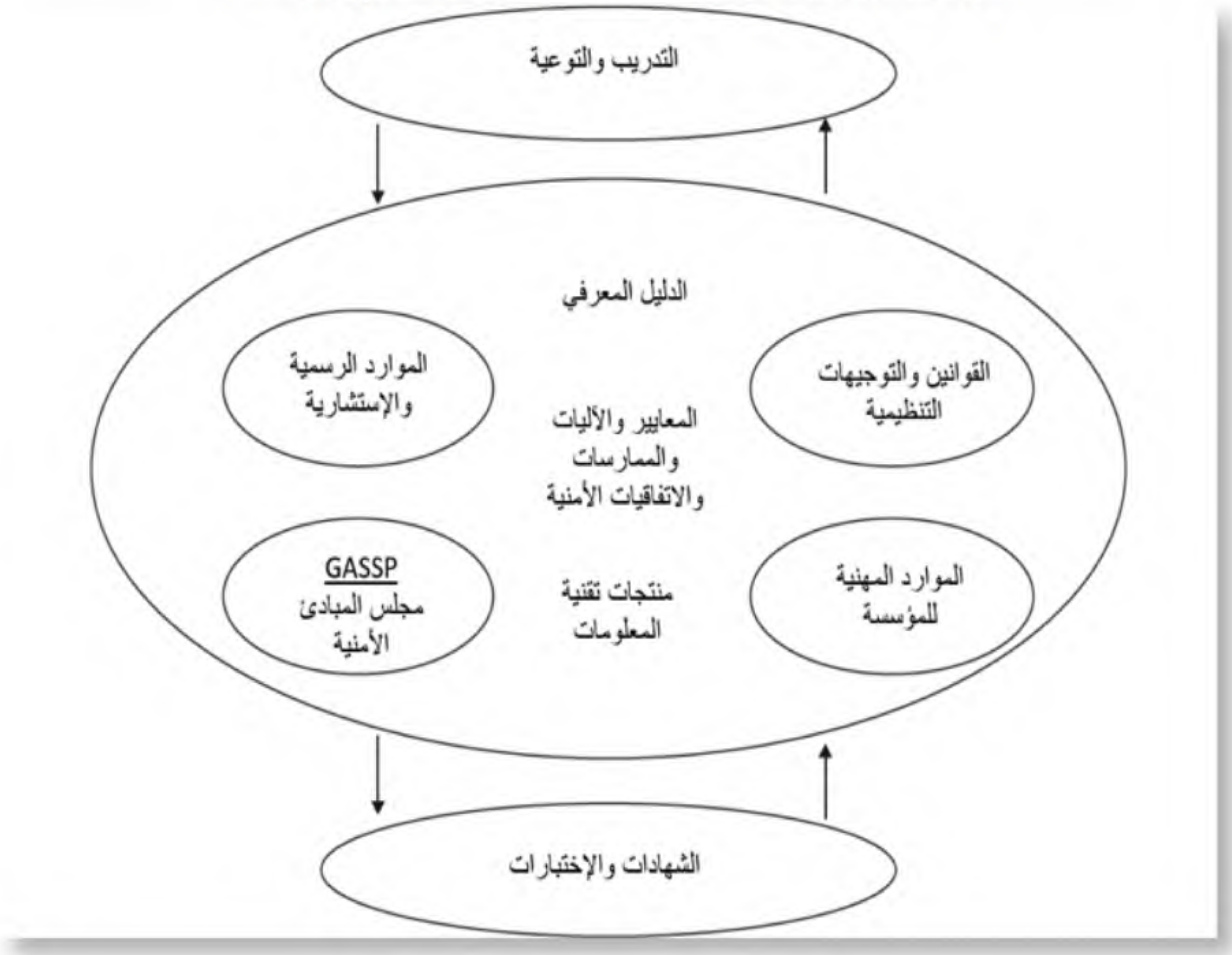
على الرغم من أن مبادئ GASSP الثمانية ليست حتمية، فإنها تلخص الإطار العام الذي يجب أن يكون أساساً للعديد من الجوانب للأمن والحوكمة الرشيدة لتقنية المعلومات. إن تجاوز تلك المبادئ يفرض على وحدة أمن تقنية المعلومات في المؤسسة إعادة التفكير ببعض الممارســات والإجراءات المتبعة حالياً لإعادة تنظيمها بشــكل يضمن تبني مبادئ GASSP. يوضح الشــكل التوضيحي (١٠-١) الدور الهام الذي تلعبه المبادئ الأمنية الرفيعة المستوى مثل GASSP في المؤسســة، مع إيلاء الاهتمام بمنتجاتها التقنية المثبتة وغيرها من العوامل. وعلى الرغم من وجود العديد من الطرق لتطبيق تلك المبادئ الأمنية، فإنه ينبغي على إدارة تقنية المعلومات ألا تفقد المسار الذي قامت عليه GASSP حيث قامت على بعض المبادئ العريضة والقوية في أمن تقنية المعلومات. وتتناول هذه المبادئ الواسعة الانتشار خصائص سرية، وســلامة، وتوافر المعلومات الخاصة بأمــن بتقنية المعلومات. كما توفر تلك المبادئ إرشادات عامة للحوكمة لإنشاء وصيانة أمن المعلومات.

سوف نتحدث عن النقاط الموضحة في الشكل التوضيحي (١٠-١) لكي نصف بإيجاز بعض العناصر الرئيســية الخاصة بمبادئ GASSP وكيفية ارتباط بعضها ببعض وبالبيئة الشــاملة لأمــن تقنيــة المعلومات. وقد تختلف أي مــن هذه المجالات أو النقاط المذكورة حســب المؤسســة وحجمها وموطنها. وســنبدأ من مركز الشــكل حيث المعايير الأمنية وغيرها من الآليات، صعوداً إلى الدليل المعرفي Body of Knowledge، ثم نسير باتجاه عقارب الساعة حول العوامل الأخرى الضرورية لتشكيل بيئة أمنية فعالة باستخدام مبادئ GASSP.

- **معايير وآليات الأمن:** نواة أي بيئة أمنية فعالة عبارة عن مجموعة من المعايير، والآليات، والممارسات، والاتفاقيات الأمنية القوية التي تخص مؤسسة ما. وهذه هي أنواع القضايا التي تمت مناقشــتها خــلال فصول هذا الكتــاب باعتبارها عمليات رقابيــة عامة فعالة لحوكمة تقنية المعلومات.

شكل توضيحي (١٠-١)

دور المبادئ رفيعة المستوى لأمن تقنية المعلومات في المؤسسة



• **الدليـــل المعرفي لمبادئ GASSP:** لقد قمنا هنـــا بتلخيص مبادئ GASSP، إلا أنه يتوجب عـــلى شريحة كبيرة ومختلفة من الأشـــخاص الذين يعملون في المؤسســـة فهم تلك المبادئ العامـــة، كما يجب عليهم أن يُظهـــروا التزامهم بفهم وتنفيذ تلك المبادئ بشـــكلٍ منتظم. الفكرة هنا هي أنه في ظل وجود أي استفسار يتعلق ببعض الممارسات الخاصة بأمن تقنية المعلومات، يتعين على إدارة تقنية المعلومات في المؤسســـة في هذه الحالة الرجوع إلى هذه المبادئ العامة لتساعدها في تفسير وحل أي قضية من القضايا التي تواجهها.

• **القوانين والتنظيمات التوجيهية:** تخضع كل مؤسسة لمجموعة متنوعة وفي الغالب مختلفة مـــن القوانـــين واللوائح التنظيمية. وخـــيرُ مثال على ذلك هنا هو أننا نســـتطيع أن نلاحظ

الاختلاف الكبير بين قوانين الخصوصية الشخصية من بلد إلى آخر. لذا يجب أن تُفسر مبادئ GASSP دائماً اعتماداً على هذه القوانين والقواعد المختلفة والمتغيرة في بعض الأوقات.

- **الموارد المهنية للمنظمة:** تقوم المنظمات المهنية مثل ISACA و AICPA بانتظام بإصدار مجموعة من الإرشادات والمعايير التي تضيف المزيد من المتطلبات الجديدة على أساليب أمن تقنية المعلومات أو تُغير من تلك الأساليب. لذا يجب على المؤسسة الإلمام بمثل هذه الأمـور ثم تقوم بعمل التغيرات المطلوبة على بيئـة أمن تقنية المعلومات الخاصة بها بما يتفق مع هذه الإرشادات والمعايير الجديدة.

- **منتجات البنية التحتية والأمنية لتقنية المعلومات:** هناك مجموعة متنوعة وواسعة من تطبيقات ومنتجات البنية التحتية لتقنية المعلومات التي تسـتطيع أن تسـاعد في عملية توجيه أو تعديل الأسـاليب الخاصة بأمن تقنية المعلومات. فبينما لا يجب على المؤسسة أن تقوم بتثبيت المنتجات التي تعاني قصوراً في هذه المبادئ الأمنية، نجد أنه من الضروري أن تكون المؤسسـة على علم بـأي خصائص جديدة وفريدة للمنتجـات التي تم تثبيتها وإجراء التعديلات المناسبة على الممارسات الأخرى لأمن تقنية المعلومات.

- **مجلـس المبادئ الأمنية الخاص بمبادئ GASSP:** عندما تقوم المؤسسـة باعتماد مبادئ GASSP، فهـي بحاجة إلى تكليف بعض الأشـخاص الموثوقين ليقوموا بتفسـير عمليات تطبيـق مبـادئ GASSP بصورة سـليمة. وقد يأتي الأشـخاص المناسـبون لهذه المهمة مـن وحدة أمـن تقنية المعلومات، أو من مجموعة ضمان الجـودة، أو ممثل عن إحدى الوحدات مثل وحدة التدقيق الداخلي لتقنية المعلومات. وعلى الرغم من أنه قد لا يكون أحد من هذه المجموعة خبيراً بمبادئ GASSP، فإن الفكرة هي تعيين شخص مسئول عن فهم تلك المبادئ يسـتطيع تفسيرها اعتماداً على الاستفسارات المطروحة ويمكن أن يكون الحَكَم إذا تطلب الأمر ذلك.

- **الموارد الرسـمية والاستشـارية:** على الرغم من أنه قد جرت العادة بعدم بيع الخدمات الاستشـارية، فإنه يجب على المؤسسـة أن تكون على ارتباط وثيق بمنظمات مهنية مثل ISACA وISC للاطـلاع على آخر التعديلات والمواد التفسـيرية الأخرى التي طرأت على مبادئ GASSP.

- **التدريــب والتوعية:** لن تكــون هناك أي قيمة حقيقية تذكر لتطبيق مبادئ GASSP في المؤسسة ما لم يكن هناك تدريب لمجموعة رئيسية من أصحاب المصلحة في هذه المؤسسة عــلى تلك المبادئ. لذا يجــب على مطوري النظم على وجه الخصــوص أن يفهموا هذه المبادئ جيداً ويستخدموها عند إطلاق التطبيقات الآمنة والفعالة للمؤسسة.
- **الشــهادات والاختبارات:** لا يوجد إلى الآن برامج خاصة بشــهادات أو اختبارات لمبادئ GASSP. غير أن مثل هذه البرامج قد يتم تطويرها في المستقبل.

ومع أن مبادئ GASSP لم تلق إلى الآن مستوى واسعاً من القبول من قِبل المؤسسات في الولايات المتحدة، ففي ظل التغيرات المســتمرة والتقدم التكنولوجي العالمي الموجود اليوم، بالإضافة إلى المخاوف المتزايدة لأمن تقنية المعلومات، توفر هذه المبادئ أساساً هاماً أو إطار عمــل للنظر في أمن تقنية المعلومات وتقييمه. لذا يجب على كبار المديرين الذين يبحثون عن طرق لإيجاد إجراءات فعالة لأمن وحوكمة تقنية المعلومات، أن ينظروا إلى تلك المبادئ على أنها نقطة بداية لتحقيق الهدف المرجو.

أهمية الإستراتيجية الأمنية الفعالة على مستوى المؤسسة:

من الممكن أن تكون هناك قيمة معتبرة نتيجة تبني مجموعة عريضة من المبادئ الأمنية مثل مبادئ GASSP، إلا أن المؤســســة بحاجة أيضاً إلى تبني وتطبيق إستراتيجية شاملة لأمن تقنية المعلومات. إن الأمن في عالم اليوم الإلكتروني والمرتكز على تقنية المعلومات يشــتمل على هياكل معقدة وتقنيات تظهر وتتطور بشــكل مســتمر. ولكي نضمن أن المؤسسة قد قامت بإنشاء مستويات مناسبة من أمن تقنية المعلومات، ينبغي عليها أن تفكر في استخدام نموذج أمني من أعلى لأسفل Top-Down لتحديد وتقييم أصولها الأمنية. فباستخدام مثل هذا النهج الأمني من أعلى لأســفل، تســتطيع الإدارة أن تدرك بشــكل أفضل مدى خطورة القضايا الخاصة بأمن تقنيــة المعلومات، ومن ثم الشروع بتطبيق العمليات التي تتبلور في الأســفل والموجودة لدى فريق عمليات التشغيل. وهذا يختلف عن النهج الذي يتبع نهجاً من أســفل إلى أعلى Bottom Up، حيث يقوم فريق تشغيلي أقل درجة ببدء العملية ومن ثم يقوم بنشر نتائجه صعوداً نحو الإدارة على شكل توصيات للسياسة المقترحة.

يقدم الشــكل التوضيحي (١٠-٢) توضيحاً بســيطاً لمفهوم النموذج الأمني من أعلى إلى أســفل Top-Down. وســتوضح الفقرات التالية عناصر هذا المفهوم بمزيد من التفصيل. وعليه فإنه يجب تطبيق البنية التحتية لأمن تقنية المعلومات بشــكل متساوٍ على الوصلات الشــبكية الموجودة مســبقاً والوصلات الجديدة للمبادرة، بعد ذلك يجب حماية الشــبكة الخاصة بالمنظمة بناء على المخاطر التي تمثلها تلك الشبكة للمنظمة.

المســتوى الأعلى من النموذج الموجود في الشكل التوضيحي (١٠-٢) يدعو إلى سياسات أمنيــة فعالــة. ومع أن الأمر قد يبدو في بعض الأحيان وكأنه واضح للغاية، فإنه ينبغي على المديــر الأول الذي يقوم بمراجعة الضوابــط الموجودة في البيئة الأمنية لتقنية المعلومات أن يقــوم بداية بتعهد فهم السياســات الأمنية الحالية لتقنية المعلومات في المؤسســة. وعلى الرغم من أن هذه السياســات تكون في العادة رفيعة المســتوى، فإن أي مجموعة سياسات كهــذه يجــب أن تُغطي الجوانب الأمنية كافة لتقنية المعلومــات. وربما يكفي أن نذكر أن السياســات الأمنية لتقنية المعلومات في المؤسسة سوف تســتند إلى المبادئ الخاصة بمعايير الآيزو التي تمت مناقشتها في الفصل السابع من هذا الكتاب وكذلك مبادئ كوبت التي تمت مناقشتها في الفصل الخامس من هذا الكتاب.

ويجــب أن تكون هذه الإســتراتيجيات الأمنية مدعومة بمعايير أمنية تفصيلية تشــمل عمليــات تنفيذ مراقبة النظــم، وتهيئة النظام للعمل كخادم تطبيقــات أو خادم ويب، أو تهيئــة الجدران النارية لفصل النظم ووضعها في مناطق محددة. كما يجب أن تكون هذه المعايير خاصة بكل من التطبيقات ونظم التشغيل، وأن تكون مفصلةً على نحوٍ كافٍ لتُمكن المســتخدم صاحب المعرفة من القيام بتنفيذ أبرز النشــاطات الموجودة في أحدٍ المعايير أو تمكنه من تهيئة النظام أو التطبيق. وأخيراً يجب على هذه المعايير أن تحدد الخطوات التي يجب اتخاذها، مثل الموافقة، في حال كان الإخلال بهذه المعايير أمراً ضرورياً.

علينــا أن نفكر في العمليات التشــغيلية لأمن تقنية المعلومات باعتبارها سلســلة من مناطق الثقة. بمعنى أنه يجب على عمليات التشــغيل الخاصة بتقنية المعلومات أن تقوم بتحديــد وتصنيف جميع الوصلات والنظم الحالية داخل الأماكن المنطقية المتعلقة بالأمن. أحد العناصر الرئيسية في هذا التصنيف الأمني هو الوصول إلى الإنترنت والوصلات الشبكية

الأخــرى مثل نظم الدعم الخاصة بالبائعين. وفيما يــلي أربعة تصنيفات ممكنة لمثل هذه النظم المتداخلة:

شكل توضيحي (١٠-٢)

مفهوم نموذج أمن تقنية المعلومات من أعلى لأسفل



١- **النظــم والعمليــات الموثوقة:** هــي النظم التي تخضــع مباشرة لســيطرة إدارة تقنية المعلومات. فمن المحتمل أن يحتاج المستخدمون والنظم إلى صلاحيات الوصول الكامل لجميع النظم الداخلية لتقنية المعلومات بشكل أساسي.

٢- **نظــم شــبه موثوقة:** هي النظم الخاصة بدعم الموردين وبعــض شركاء الأعمال. والتي تحتاج إلى صلاحيات وصول موثوقة لحماية النظم المكشوفة التي لا تكون متاحة لعامة الناس.

٣- **نظــم غير موثوقة:** هــي غالباً النظم والعمليات المرتبطة بالعميل والتي تتطلب حقوق وصول موثوقة لمصادر معلومات محددة. هذا بالإضافة إلى النظم المكشــوفة والمتاحة لعامة الناس.

٤- **النظم العدائية وتهديدات العملية:** حقوق وصول مقيدة ومحددة جداً فقط هي التي يُسمح بها للوصول إلى مثل هذه النظم. وينبغي الكشف عن محاولات الوصول غير المصرح بها في الوقت الحقيقي.

عقب هذه التصنيفات، لا بد من إعادة النظر في جيمع المستويات الخاصة بروابط أو علاقات تقنية المعلومات مثل دعم الموردين والعملاء والشركات الفرعية التابعة وشركاء الأعمال ووضعها على مستوى من الثقة وفقاً لأنواع الضوابط التي يمكن المحافظة عليها. فضلاً عن أن تحديد كل رابط في منظمة كبيرة يمكن أن يكون في أحسن الأحوال أمراً صعباً. من الوسائل الفعالة لعمل تصنيف كهذا هو القيام بعقد ورشة عمل يشارك فيها مجموعة كبيرة من أعضاء طاقم العمل ذوي المعرفة والاطلاع المدركين للمفاهيم المرتبطة بأعمال المؤسسة والمشاريع وعلى علم بالمشاريع الأخرى داخل المؤسسة وبعمليات التشغيل الخاصة بتقنية المعلومات فيها. ومع أنه من غير المرجح تحديد الروابط كافة في ورشة عمل واحدة، فإن هذا النوع من الممارسة قد يساعد على تحديد أغلبية الروابط، ويساعد أيضاً على تحديد أعضاء طاقم العمل الآخرين في المؤسسة الذين قد يكونون مسؤولين عن تحديد تلك الروابط وغيرها.

لا بد من توثيق هذه الروابط أو العلاقات وكذلك بروتوكولات الاتصالات الشبكية الخاصة بها واستخدامها لوضع ضوابط تفصيلية للسماح بالوصول من المواقع المناسبة المقصودة وإليها. ونتيجة لذلك فإنه ينبغي على المؤسسة الفصل بين الأجزاء المختلفة من شبكتها إلى عدة مناطق ثقة.

إن عملية فصل وتصنيف النظم والعمليات تعمل على فصل النظم اعتماداً على فئات محددة من الثقة. لذا يجب أن يكون هناك دائماً لدى الشبكة الداخلية لتقنية المعلومات في المؤسسة الجزء الشبكي الخاصة بها، مشتملاً على خادم الويب، وخادم البريد الإلكتروني، وخادم اسم النطاق وغيرها من الخوادم الأخرى التي يجب أن يتم تصنيفها إلى مناطق ثقة وأن يتم تقسيمها أو تجزئتها بشكل مناسب. قد يؤدي هذا إلى تجزئة كل خدمة من هذه الخدمات ووضعها في مناطق منفصلة أو قد يؤدي إلى تنفيذ عدد من هذه الخدمات في منطقة واحدة. وسيعتمد التصميم النهائي للهيكل الأمني المحيط على هذا التصنيف الخاص

بالنظــم والخدمات، غير أن تصميم تلك المناطق والتصنيفات يعد أحد العناصر الحساســة للأمن المحيط بتقنية المعلومات.

تخطيط استمرارية تقنية المعلومات:

على مر السنين وخاصة في زمن استخدام الحواسيب المركزية القديمة، كان مدققو تقنية المعلومات في المؤسســة يقومون غالباً بإثارة العديد من القضايا التي تتعلق بمخاطر فقدان المؤسســة لقســم كبير من مواردها الخاصة بتقنية المعلومات نتيجة وقوع أحداث كارثية. الأمــر الذي كان مصدر قلق كبير، وخصوصــاً في الأيام الأولى لظهور تقنية المعلومات عندما كانــت معظم العمليات التشــغيلية للنظــم تعتمد على النظم المركزيــة، حيث كان هناك القليل من وصلات الاتصالات لربط الموارد الخاصة بتقنية المعلومات، وقد كان يتم في هذه النظم المركزية القديمة تثبيت جميع التركيبات المطلوبة تقريباً من قبل البائع، إذ إن تركيب نظام جديد كان يستلزم جهوداً ضخمة.

وقــد أدركت الإدارة العليا لاحقــاً مخاطر تعطل تلك النظم، واســتجابة لتلك المخاوف قامــت أقســام تقنية المعلومات بتطوير إســتراتيجيات بديلة للمعالجــة. إن هذا التطوير الــذي حدث في النظام والذي أصبح يعرف باســم التخطيط للتعافي مــن الكوارث الخاصة بتقنية المعلومات، وفيه ستقوم المؤسسة غالباً بعمل الترتيبات اللازمة لتجهيز الموقع البديل الخاص بالمعالجة لتغطية مخاطر تَعطل النظام المركزي. ونظراً لأن تنفيذ مثل هذه الخطط قــد يكون مكلفــاً، فإن مديري التدقيق الداخلي وغيرهم مــن المديرين في كثير من الأحيان كانت لديهم صعوبة في الترويج وتنبيه الإدارة العليا من تلك المخاطر. يسترجع مؤلف هذا الكتــاب ذكرياته عندما كان يدير إحدى عمليات تدقيق تقنية المعلومات الخاصة بتخطيط التعافي من الكوارث لإحدى الشركات التي أصبحت فيما بعد من أكبر الشركات الأمريكية في مطلع التسعينيات من القرن الماضي، حيث كان واحد من المراكز الرئيسية للبيانات الخاصة بالشركــة يقع بالقرب مــن أحد المطارات المزدحم بحركات الطائــرات - مع وجود مخاطرة تتعلــق بوقوع حــوادث طيران - حيث لم تكــن هناك أي خطة فعالة جاهــزة للتعافي من الكوارث. وعندما قام قســم التدقيق الداخلي وللمرة الأولى بإثارة المخاوف المتعلقة بعدم وجود خطة فعالة لاسترجاع تقنية المعلومات، قام وقتها الرئيس التنفيذي للمعلومات CIO

بتجاهل هذه المخاوف قائلاً إن مثل هذه الكوارث لا يمكن أن تحدث أبداً. وفي النهاية قام هــذا المؤلف مع إدارة التدقيق الداخلي بإثــارة تلك المخاوف في أحد الاجتماعات مع لجنة التدقيق لتهيئة الشركة لإطلاق مثل هذه الجهود الخاصة بالتخطيط لمواجهة الكوارث.

خــلال الفــترة من ثمانينيات وحتى مطلع تســعينيات القرن الماضي، كان الحل الشــائع للتعافي من الكوارث المتعلقة بتقنية المعلومات بالنســبة للمؤسســات الكبيرة هو التنسيق مــع أحد المرافق البعيدة المخصصة لمعالجة بيانات التعــافي من الكوارث لإجراء المعالجات الطارئة. وقد تم تخزين نســخ احتياطية للملفات والبرامج الرئيسية في أماكن خارج موقع العمل الحالي. مع وجود خطط تدعو موظفي تقنية المعلومات إلى التحول لاســتخدام تلك المرافــق البديلــة في حال وقوع الكوارث. اعتقد المهنيون أن كــوارث تقنية المعلومات هي فقــط الحرائق والفيضانات أو بعض أحوال الطقس الســيئة الأخــرى. في تلك الأيام الأولى لنظم الحاســبات المركزية القديمة، كانت الشركات تســتخدم في بعــض الأحيان ما يبدو لنا اليوم وكأنها طرق غريبة لتطوير خططها الخاصة بالتعافي من كوارث تقنية المعلومات. فقد كانــت هذه الطرق تقوم على توقيع "اتفاقيات تبادلية" مع مواقع قريبة منها ولديها موارد تقنيــة مماثلة لمواردها بحيث يمكن لكل منهــما أن ينتقل إلى موقع آخر للمعالجة في حال وقــع طارئ ما عند أي طرف من الطرفين. إن توقيع اتفاقية تبادلية بين اثنين من المديرين التنفيذيــين للمعلومــات CIOs يبدو أمراً جيداً من الناحية النظريــة، إلا أنها في الواقع لن تقدم أكثر من مجرد مساعدة إنسانية بشكل أساسي. فربما يكون هذا الموقع القريب الذي تــم إبــرام اتفاقية تبادلية مع القائمين عليه خارج نطاق الخدمة أيضاً للســبب نفســه من الكوارث الطبيعية المتعلقة بالطقس، أو ربما لن يهتم بأي طرف آخر يقوم بتشــغيل النظم الخاصة به في فترات خارج ورديات العمل. وكعائق أخير، فإن المستشار القانوني للشركة قد يكون لديه مجموعة من الأسباب ليقول لا للاتفاقية التبادلية.

في السابق، حيث كان يتم وضع نظم الحاسبات المركزية في مرافق بالأدوار العليا وكانت هناك مساحة للكوابل وغيرها من المعدات الأخرى الموضوعة في الطابق نفسه، وكان هناك عــدد محدود من الموردين (مثل IBM، Amdahl, Univac ، وقليل غيرهم) هم فقط من يقومون بتركيب وإعداد معظم النظم الخاصة بالحاســبات المركزية تقريباً. لذا فإن عملية

الانتقال إلى نظام بديل في الحالات الطارئة كانت تشكل تحدياً كبيراً. في الحقيقة، إن القيام بهذه العملية اليوم أصبح أسهل بكثير، إذ تكون معدات الحاسب في العادة جاهزة للعمل بدلاً من تلك التي تحتاج إلى تصنيع وتهيئة مخصصة، كما كان شائعاً في الماضي.

لم تكن الخطط الأولى للتعافي من الكوارث دقيقة بدرجة كبيرة. إلا أنه سرعان ما ظهرت مجموعة من بائعي أدوات التعافي من الكوارث الذين لديهم مواقع لنظم الحاسب مجهزة بالكامل والتي تكون متوقفة عن العمل (أو ما كان يسمى بالمواقع "الساخنة" "hot" Sites) لتعمل بصفة مرفق احتياطي في حالة الطوارئ. في تلك الأيام الخاصة بالمرافق المركزية لتقنية المعلومات، كانت الشركات تتعاقد غالباً لاستخدام تلك المواقع "الساخنة" مرافق لها للتعافي من الكوارث، وإجراء الاختبارات الدورية، والاحتفاظ هناك بنسخ احتياطية من الملفات الرئيسية لذا كان على إدارة تقنية المعلومات إعادة التفكير في إستراتيجياتها.

أما في عصرنا الحالي الذي يتميز بالبيئة الافتراضية للتخزين في نظام الخادم-العميل والتطبيقات القائمة على شبكة الإنترنت (تطبيقات الويب) فإن المؤسسة أصبحت تواجه مجموعة جديدة من المخاطر المحيطة بأصول تقنية المعلومات الخاصة بها. فمن الطبيعي ألا يكون هناك جهاز مركزي واحد للتعامل مع التطبيقات الآلية الكبيرة، وإنما يوجد مجموعة واسعة من أجهزة الحاسب المكتبية والخوادم والتسهيلات السحابية وغيرها من النظم المتصلة عادة من خلال وسائل اتصال بالغة التعقيد، وشبكات لإدارة التخزين، وروابط مع الإنترنت. إن المؤسسات لا تضع كافة موارد تقنية المعلومات الخاصة بها تقريباً في مركز بيانات واحد (أو أكثر)، فالإدارة مهتمة بالإبقاء على مرافق تقنية المعلومات الخاصة بها تعمل على أكمل وجه أكثر من قلقها بشأن المخاطر المتعلقة بفقدان أحد مرافق نظم الحاسب المركزية. إن المبدأ الأساسي للتخطيط من أجل التعافي من كوارث تقنية المعلومات كان يعتمد على امتلاك عمليات معمول بها لاستئناف عمليات التشغيل في حال حدثت كارثة ما، يمكن أن تتسبب في تعطيل مركز الحاسب. إن هذا النهج القديم للتعافي من الكوارث لم يعد صالحاً اليوم. فالمؤسسة بحاجة للتخطيط لاستمرارية العمليات التشغيلية لأعمالها في حال التعرض لأحداث غير متوقعة.

فمـع وجود نظم الخادم والنظم القائمة على الإنترنت اليوم، نجد أن اللغة والأسـاليب الإسـتراتيجية الخاصة بتخطيط اسـتمرارية الأعمال والتعافي من كـوارث تقنية المعلومات قد تغيرت. لذا يتعين على المهنيين الآن التفكير في أهمية وجود خطة لاسـتمرارية الأعمال Business Continuity Plan (BCP) والتـي تتكون من الإجراءات والعمليات الضرورية التي يجب اتباعها لاسـتعادة كل العمليات التشغيلية للأعمال. إن النهج والمطلب الجديد هو وضع خطة لاسـتمرارية الأعمال BCP بدلاً من وضـع خطة للتعافي من الكوارث التي كانت موجودة في السـابق. فالمستخدم الذي يقوم باستخدام أحد النظم الخاصة بمعالجة طلبـات الشراء عبر الإنترنت تكون درجة اهتمامه بحالة الخـادم فيما إذا كان يعمل أو لا أقل من اهتمامه بطلب العميل الذي تم تسليمه عبر موقع الإنترنت فيما إن كان قد تمت معالجته بشـكل سـليم وفعال أم لا. لذا يجب استعادة وتشـغيل التطبيق بشكل سريع وفعال قدر الإمكان، إلا أنه يبقى الهدف الرئيسي وهو دعم واستعادة عمليات الأعمال.

خطط استمرارية الأعمال وحوكمة تقنية المعلومات:

لا يزال بعـض مديري تقنية المعلومات ينظرون إلى المخاطـر والتعافي من الكوارث من منظور الخطة التقليدية القديمة للتعافي من الكوارث، على الرغم من أن تلك الخطط كانت تعتمد على الحاسـبات المركزيـة القديمة والتي كانت موجودة قبـل ظهور الإنترنت بزمن بعيد. في الأيام الأولى لتقنية المعلومات كان هناك تركيز كبير على مسـألة التخطيط للتعافي من الكوارث - أي اسـتعادة نظم أجهزة الحاسـب والتطبيقات وملفـات البيانات الخاصة بتقنية المعلومات - أما اسـترجاع العمليات الأساسـية للأعمال فلم تُعط الدرجة نفسها من الاهتـمام. وعلى الرغم من أن التعافي من كوارث تقنية المعلومات لايزال من الأمور الهامة، إلا أن الإجراءات والممارسـات الفعالة التي كانت مستخدمة سابقاً للتعافي من كوارث تقنية المعلومـات تكون غالباً ذات قيمة محـدودة في ظل عالم اليوم المتصـل بالإنترنت، والنظم القائمة على الحوسبة السحابية الموجودة حالياً. ولكي تقوم المؤسسة بدعم عمليات حوكمة تقنية المعلومات الخاصة بها يجب أن تقوم بتثبيت وتنفيذ خطة شـاملة قوية لاسـتمرارية الأعمال BCP تشمل كلاً من استرجاع النظم وعمليات الأعمال الخاصة بها.

بالنسـبة لبعض المهنيين، فإن هذه المصطلحـات يكتنفها بعض الغموض. فعند البحث في الويب سـواء عن "التعـافي من كوارث تقنيـة المعلومـات IT disaster recovery" أو "خطة الاسـتمرارية Continuity Planning" سوف يقدم هذا البحث خليطاً من المراجع المتباينة لكلا المفهومين، متجاهلاً ما نعتبره فروقاً جوهرية بين هذين المجالين. فمعظم هذه المراجع، على الرغم من أسمائها، فهي تركز على التخطيط التقليدي للتعافي من كوارث تقنية المعلومات بدلاً مـن العمليات الأكثر عمومية والخاصة بخطط اسـتمرارية الأعمال BCP. وفي مثـال عـلى هذا اللبس، قامت إحـدى المنظمات المهنية ذات مرة بإطلاق اسـم معهد التعافي من الكـوارث Disaster Recovery Institute (DRI) على معهد إدارة الطوارئ[٤] Institute for Contingency Management وهو الاسم الذي يعرف به حالياً.

ينبغي على كل مؤسسـة أن تمتلك خطة فعالة ومعمولاً بها لاسـتمرارية الأعمال BCP بصرف النظر عن حجم العمليات التشغيلية أو مدى أهمية موارد تقنية المعلومات الخاصة بها. مع تركيز هذه الخطة على الأشـخاص والمرافـق المادية وغيرها من الموارد، فإن إطلاق خطة فعالة لاسـتمرارية الأعمال BCP يتطلب مشـاركة طيف عريض من مديري المؤسسة وغيرهم من العاملين. من ناحية أخرى تمثل موارد تقنية المعلومات أحد العناصر الأساسية في خطة استمرارية الأعمال BCP، ولهذا السبب يجب على إدارة المؤسسة أن تدرك وتلعب دوراً أساسياً في ترسيخ خطة استمرارية الأعمال BCP في المؤسسة.

وتمتـد الخطة الفعالة لاسـتمرارية الأعمال BCP إلى ما هو أبعـد من تقنية المعلومات لتشمل اسـتعادة واستئناف جميع العمليات التشغيلية في المؤسسة والحفاظ عليها. وعلى الرغـم من أن اسـتعادة نظم تقنية المعلومـات والبيانات الإلكترونية يعد أمـراً هاماً، فإن اسـترجاع تلك النظم والبيانات لن يكون كافياً دائماً لاسـتعادة عمليات التشـغيل الخاصة بالأعـمال. فهنـاك العديد مـن الجوانب المتعلقة باسـتمرارية الأعمال مثـل وضع خطة الاسـتجابة في حال حدوث فيضانات غير متوقعة أثناء عملية اسـتخراج المعادن. على كل حال فإن الحديث في هذا الفصل سيكون عن العمليات التشغيلية للأعمال مع دعم مكثف للعمليات التشغيلية لتقنية المعلومات.

وتشتمل خطة استمرارية الأعمال BCP في المؤسسة على تحديد أولويات أهداف الأعمال وعمليات التشغيل الحرجة ، والتي تعد من الأمور الأساسية لعملية التعافي. لذلك لابد من هيكلة العمليات ضمن إطار عمل على مستوى المؤسسة يأخذ بعين الاعتبار جميع العمليات الهامة ووحدات الأعمال والإدارات والنظم المطلوبة للاستجابة للحلول الخاصة بالخلل والتعافي التي يجب تطبيقها. كما يجب أن يشتمل هذا الإطار على خطة قصيرة وطويلة المدى لعمليات التشغيل الخاصة بالاسترجاع، فبدون العمليات الخاصة بخطة استمرارية الأعمال BCP على مستوى المؤسسة التي تأخذ بعين الاعتبار جميع عناصر الأعمال الحساسة؛ ربما يجعل المؤسسة غير قادرة على استئناف الخدمات التي تقدم للعملاء وغيرها من عمليات التشغيل عند مستويات مقبولة. ومع أن العديد من مؤسسات اليوم تفتقر غالباً إلى وجود خطط كهذه، فإنه يجب على الإدارة أن تقوم بتحديد أولويات الأهداف الخاصة بأعمالها وعمليات التشغيل الحساسة لديها والتي تعد من الأمور الأساسية لبقاء المؤسسة، وذلك على اعتبار أن استعادة جميع وحدات الأعمال قد لا يكون ممكناً بسبب التكلفة، وخدمات الإمداد أو التجهيزات، وظروف أخرى غير متوقعة.

كما يجب أن تشتمل خطة استمرارية الأعمال BCP الفعالة على تحديث منتظم لتلك الخطة بناء على عمليات الأعمال وتوصيات التدقيق والدروس المستفادة من عملية الاختبار. وتشتمل التغيرات في عمليات الأعمال على التطورات التقنية التي تسمح بمعالجة أسرع وأكثر كفاءة، والتي من خلالها يتم تقليل الفترات المقبولة لاسترجاع العملية الخاصة بالأعمال. واستجابة للمطالب التنافسية ورغبات العملاء، فإن العديد من المؤسسات تقترب من فترات أقل للتعافي وتصميم حلول تقنية للتعافي داخل عمليات الأعمال. هذه التطورات التقنية تشدد على أهمية صيانة خطة استمرارية الأعمال BCP على مستوى المؤسسة والحفاظ عليها.

وفضلاً عن أنه قد يوجد العديد من الاختلافات في عمليات التشغيل الخاصة بالأعمال المؤسسية، والعديد من الاختلافات التي تحتاج المؤسسة إلى أن تقوم بها من أجل تحقيق الاستمرارية في حالة وقوع بعض الحوادث أو الكوارث غير المتوقعة؛ فإنه من الصعب وضع وصف تفصيلي للمعايير الخاصة بخطة استمرارية الأعمال BCP. ولتطبيق خطة لاستمرارية

الأعمال BCP، يجب على إدارة المؤسسة أن تأخذ بعين الاعتبار الإرشادات المتعلقة باستمرارية الأعمال التي تم تطويرها بواسطة منظمات مهنية مختلفة كالجمعية الوطنية الأمريكية للحماية من الحريق (National Fire Protection Association (NFPA، التي تم تطويرها من خلال بائعي الحاسبات كشركة أوراكل Oracle وإتش بي HP، أو التي تم تطويرها من خلال منظمات المعايير الوطنية الأخرى. ولعل أفضل المواد الخاصة بأفضل الممارسات المتبعة لاستمرارية الأعمال وأكثرها شهرة، هي التي صدرت عن الهيئة البريطانية الوطنية للمعايير (www.bsi.gove.uk (BSI ومعهد استمرارية الأعمال التابع لها الذي يقوم بنشر إرشادات حول بعض الممارسات الجيدة. هذه المعايير مشابهة لمعايير الآيزو ISO التي تمت مناقشتها في الفصل السابع من هذا الكتاب. ويوضح الشكل التوضيحي (١٠-٣) نظرة عامة حول دورة حياة خطة استمرارية الأعمال BCP وفقاً للمعيار البريطاني BS 25999.

لقد قمنا بوصف هذا النهج الخاص بخطة استمرارية الأعمال BCP على أنها عملية حلقية ومستمرة لدورة الحياة، في وسط هذه العملية يوجد ما يعرف بإدارة برنامج خطة استمرارية الأعمال BCP وفي خطوة أولى لإصدار خطة فعالة لاستمرارية الأعمال، يجب على المدير المسؤول في المؤسسة أن يتحمل مسؤولية تعريف وإدارة البرنامج الخاص بوضع خطة استمرارية الأعمال BCP. لقد كانت المؤسسات على مر التاريخ تنظر إلى قسم تقنية المعلومات التابع لها وتفترض أن العاملين بهذا القسم سيقومون بإدارة العمليات التشغيلية الخاصة بخطة استمرارية الأعمال BCP باعتبار أنه الفريق المسؤول عن خطة التعافي من كوارث تقنية المعلومات وعمليات النسخ الاحتياطي للملفات والاختبارات الدورية لهذه الخطة. فضلاً عن أنه في الغالب توجد عمليات ومهام أخرى تخص الاستمرارية تذهب إلى ما هو أبعد من مجرد تقنية المعلومات، كما أن هناك آخرين في المؤسسة ربما يكونون هم الأطراف الأكثر ملاءمة للاضطلاع بمسؤولية هذا البرنامج على مستوى المؤسسة.

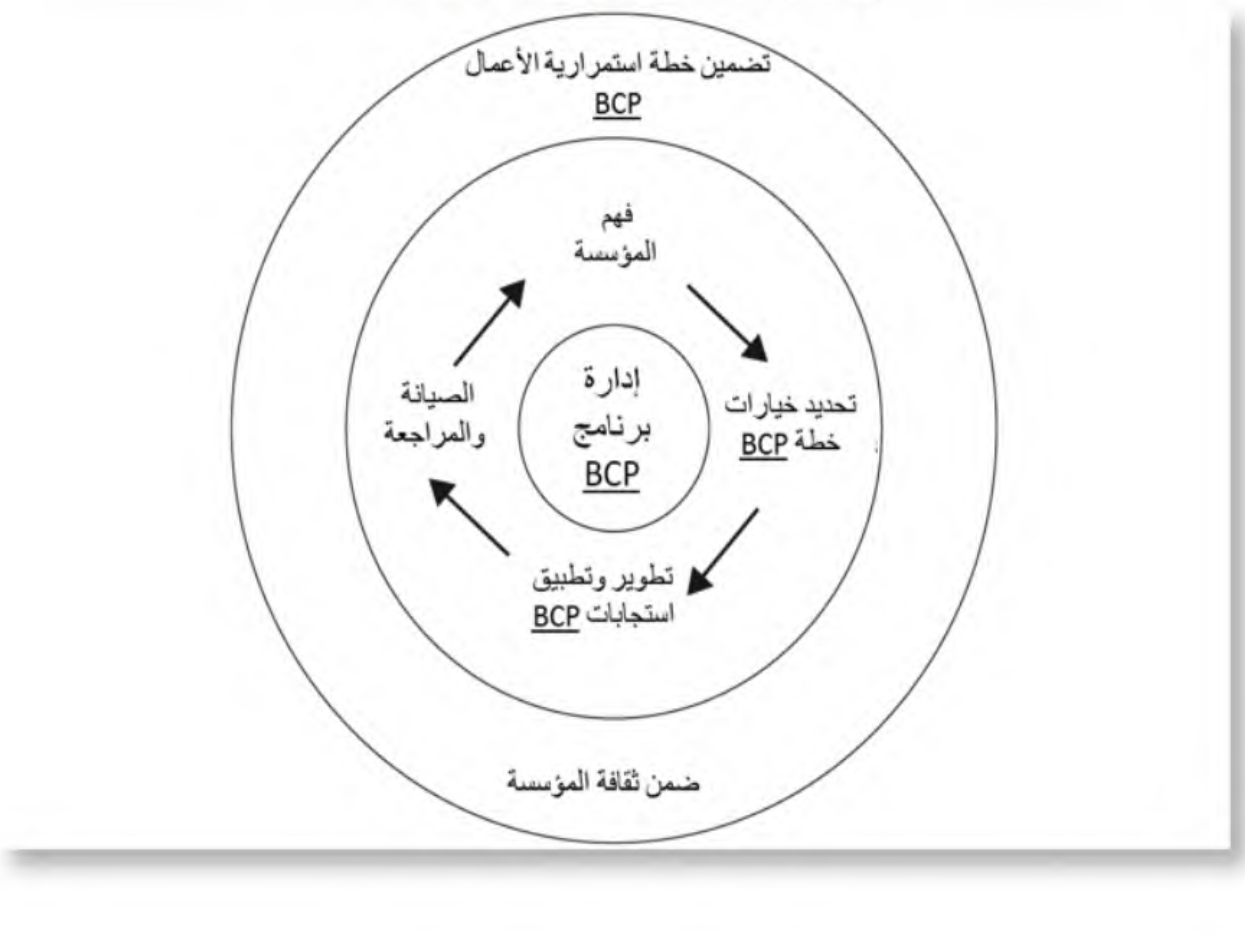
أما في المؤسسات التي يوجد بها وحدة لإدارة المخاطر، يكون المدير التنفيذي للمخاطر عادة هو الشخص الأنسب لتحمل مسؤولية برنامج إعداد خطة استمرارية الأعمال BCP. لكن في حالات أخرى، فإن المدير التنفيذي للمعلومات CIO يمكن أن يتحمل كامل المسؤولية، أو قد يتم إسناد المهمة هنا إلى إدارة ضمان الجودة في المؤسسة. وتعد

خطة اســتمرارية الأعمال BCP أحد العنــاصر الهامة للغاية في حوكمة تقنية المعلومات في المؤسســة. وفي جميع الحالات فإنه ينبغي على لجنة التدقيق أن تقوم بمراجعة إستراتيجية خطة استمرارية الأعمال BCP هذه والموافقة عليها.

أضــف إلى ذلك أن المؤسســة تحتاج إلى وضع سياســة رفيعة المســتوى لتحديد نطاق وأهداف خطط اســتمرارية الأعمال BCPs الخاصة بها. فمن الســهل على المدير الأول أن يصرح بأن خطة اســتمرارية الأعمال BCP لدى المؤسســة ستغطي كل شيء، غير أن هناك حاجة لمحددات رفيعة المستوى تتعلق بنطاق الخطة. وعلى الرغم من أن تصريحات كهذه قــد تبدو رائعة ومثيرة للإعجاب، فإنه قد يكون هناك منتجات أو خدمات معينة لا تحتاج إلى أن تكون في أي مستوى من المستويات العليا في خطط استمرارية الأعمال BCP.

شكل توضيحي (١٠-٣)

دورة حياة خطة استمرارية الأعمال BCP



لابد من تأسيس فريق يعمل تحت إدارة الوحدة المؤسسية التي أُسندت إليها مسئولية إعداد خطة استمرارية الأعمال BCP الخاصة بالمؤسسة. مهمة هذا الفريق تطوير سياسة استمرارية الأعمال للمؤسسة. بحيث تشتمل هذه السياسة على ما يلي:

- مراجعة أي مواد حالية متعلقة بالتخطيط لاستمرارية الأعمال في المؤسسة مثل الخطط الموجودة للتعافي من كوارث تقنية المعلومات أو خطط الطوارئ المتعلقة بالأحوال الجوية. وذلك لتحديد مدى ملاءمة الإجراءات الخاصة بخطة استمرارية الأعمال BCP الخاصة بها .
- تحديد أي من إرشادات الممارسات الجيدة أو التنظيمات أو التشريعات التي يجب تضمينها في أي خطة لإدارة استمرارية الأعمال BCM.
- إجراء تقييم رفيع المستوى للمخاطر المتعلقة بخطة استمرارية الأعمال BCP، بمعنى، تحديد جميع النظم الرئيسية وخطوط الإنتاج ووحدات الأعمال وغيرها من الإدارات التي تتطلب أولويات عليا لاستمرارية أعمالها
- تطوير سياسة المؤسسة لاستمرارية الأعمال ومناقشة فرضياتها للحصول على موافقة الإدارة العليا ولجنة التدقيق.
- نشر السياسة التي تمت الموافقة عليها لخطة استمرارية الأعمال BCP على أنها دليل رفيع المستوى لإطلاق البرنامج الشامل لاستمرارية أعمال المؤسسة.

يجب أن تصبح هذه الخطة المتفق عليها أو المقبولة لاستمرارية الأعمال BCP فيما بعد بمثابة حجر الأساس لجميع أنشطة التخطيط لاستمرارية المؤسسة. وهذا هو جوهر مفهوم الحوكمة الذي سوف يسمح للمؤسسة بتضمين خطط استمرارية الأعمال في ثقافتها العامة. كما يجب استخدامها من قبل المواد الإرشادية الخاصة باستمرارية الأعمال التي تمت مناقشتها في هذا الفصل في خطوة أولية لإطلاق مجموعة من العمليات الفعالة لإدارة استمرارية الأعمال (Business Continuity Management (BCM. وكما ذكرنا سابقاً، لا بد أن نرى هذا القالب، أو نمطاً قريباً جداً منه في أقرب وقت ممكن، وقد أصبح معياراً عالمياً لعملية استمرارية الأعمال، تماماً كإطار عمل الرقابة الداخلية الصادر عن لجنة

المنظمات الراعية (COSO) الذي تمت مناقشـته في الفصل الرابع من هذا الكتاب والذي أصبح معياراً عالمياً.

يلخص نموذج دورة حياة إدارة استمرارية الأعمال BCM الموضح في الشكل التوضيحي (١٠-٣) العمليـات الضروريـة لفهـم التنظيم النمطي للأعمال. ونتيجـة لذلك يجب أن تكون المؤسسـة في وضع يمكنها من اختيار إسـتراتيجيات ملائمة لاستمرارية أعمالها حتى تتمكـن مـن تحقيق الأهداف المرجـوة من وضع خطة لاسـتمرارية الأعمال BCP. كما يجب على المؤسسـة إطلاق مجموعة من العمليات البديلة للتشغيل لكي يتم استخدامها بعـد الانقطـاع الناتج عن عطل ما وذلك للإبقاء على أنشـطة الأعـمال في كل مجال من المجالات الرئيسية. وبناء على المخاطر التي تم تقديرها، فإن هذه الإستراتيجيات يجب أن تعتمد على مجموعة من العوامل، في تحديد أطول فترة زمنية مسـموح بها لتوقف بعض الأنشطة الحرجة، وتكلفة تطبيق الإستراتيجية بالإضافة إلى العواقب الناتجة عن أي عطل أو انقطاع.

إن الفـرق الجوهري بين اتباع هـذا النموذج الخاص بخطة اسـتمرارية الأعمال BCP والطرق التقليدية القديمة للتعافي من الكوارث، هو أن المخططين يجب أن لا يفكروا بخطة إستراتيجية واحدة للمؤسسة فحسب، بل لا بد من التفكير في كثير من الطرق المختلفة على مستوى النشاط بالنسبة للمؤسسة. إن التعقيدية الخاصة بالاعتمادات المتبادلة فيما يتعلق بالخدمـات، وعمليات الأعمال، والبيانـات، والتقنيات تحتـاج إلى تحليل، وذلك من خلال الوسائل المناسبة لمعالجة احتياجات كل من:

- **الأشـخاص في المؤسسـة:** هناك حاجة لتحديد إستراتيجيات ملائمة للحفاظ على المهارات والمعرفة الأساسـية للأفراد داخل المؤسسـة ومسـتوى المعرفة لدى الأشخاص العاملين في المؤسسة والحفاظ عليها. فالعديد من هذه الاحتياجات هنا تشمل مجالات مثل أوصاف وظيفية موثقة، تدرج في التخطيط، والعديد من الممارسـات الأخرى التي يجب تعزيزها من قبل الإدارة الجيدة للموارد البشرية. من ناحية أخرى يجب أن تدرك إسـتراتيجيات الأعمال دائماً أن الأفراد الأساسـيين قد لا يكونون متاحين لمواصلة النشـاط، وأن عمليات الاستمرارية القائمة على الأفراد يجب أن تكون دائماً في موضع التنفيذ.

- **احتياجات موقع العمل:** يجب على المؤسسة وضع إستراتيجية للتقليل من الآثار المترتبة على عدم إتاحة مواقع العمل الطبيعية. ويتطلب ذلك في معظم الحالات إستراتيجية لتحديد مواقع بديلة لاستمرار العمليات التشغيلية أو حتى تحديد أحد الموظفين للعمل من المنزل للقيام ببعض الأنشطة. فإذا كانت بعض مرافق المؤسسة قد تم تضمينها في أنشطة مثل الصناعات الثقيلة أو المعالجة الكيميائية، مهما يكن، فإن إتاحة موقع بديل ربما لا يكون بالأمر السهل، بل إن إستراتيجيات أخرى على مستوى النشاط قد تتضمن حتى الانسحاب من عمليات التشغيل على المدى القصير.

- **التقنيات الداعمة:** تعتمد المؤسسات على مرافق تقنية المعلومات ومعالجات شبكة الاتصالات السلكية واللاسلكية وموارد فحص المنتجات وعلى العديد من الأجهزة الأخرى حسب المنتج أو النشاط. وعلى الرغم من أن العديد من المؤسسات قد قامت بالفعل بتطوير خطط قوية للتعافي من كوارث تقنية المعلومات، فإن هذه المؤسسات بحاجة إلى فهم الأنشطة الأخرى لديها والقائمة على التقنية بشكل جيد لتقوم بتطوير إستراتيجيات مناسبة لخطط استمرارية الأعمال BCP.

- **المعلومات الفعلية والافتراضية:** بالإضافة إلى موارد تقنية المعلومات وغيرها من الأدوات القائمة على التقنية، يجب أن يكون لدى المؤسسة مجموعة كبيرة من الأنشطة المتعلقة بالمعلومات التي يمكن تقديمها على هيئة نسخ حقيقية وكذلك نسخ افتراضية أو إلكترونية. كما يجب أن يكون لأي معلومة مطلوبة لتنفيذ أنشطة حساسة الضوابط الملائمة والخاصة بالسرية والنزاهة والإتاحة والتداول.

- **المعدات والأجهزة:** يجب على المؤسسة تحديد وحيازة مخزون الأجهزة والمعدات الأساسية التي تدعم الأنشطة الحساسة. فقد تتضمن الإستراتيجيات القائمة على النشاط تخزين الأجهزة في مواقع بديلة، أو عمل الترتيبات اللازمة مع الأطراف الثالثة لتسليم الأجهزة، أو حيازة أجهزة معينة في مستودعات منفصلة، أو تحديد مصادر توريد بديلة. ولأن الأنشطة الحساسة تعتمد على تجهيزات متخصصة، يجب تحديد أو إجراء الاستعدادات التعاقدية مع الموردين الرئيسيين الحاليين.

- **أصحـاب المصالح والشركاء والمقاولون:** يجب على المؤسســة وضع اســتراتيجيات ملائمة لإدارة العلاقات مع أصحاب المصالح وشركاء الأعمال أو الخدمات والمقاولين الرئيسين، لذا يجب على إستراتيجية إدارة استمرارية الأعمال BCM أن تأخذ بعين الاعتبار تلك الأطراف المعنية الرئيسية والعمل على حماية مصالحهم.

إن تطوير خطة استمرارية الأعمال والإستراتيجية الداعمة قد يكون في الواقع جهداً كبيراً لتغطية جميع أنشطة المؤسسة. لذا يجب على الخطة الشاملة لاستمرارية الأعمال BCP أن تنظر في جميع التهديدات الخاصة بالاســتمرارية فيما يتعلق بالروابط والعلاقات بين جميع الأنشــطة الرئيســية للمؤسســة. ونظراً لكثرة التداخلات في جميع أنواع عمليات التشغيل الخاصة بالأعمال، فإن هناك عدداً قليلاً قائماً بذاته، وأنشطة مستقلة تماماً.

إن الممارســات الفعالة لأمن تقنيــة المعلومات عبارة عن مجموعة مــن المهام المعقدة والتي تتطلب دعماً فنياً قوياً لتقنية المعلومات في المؤسسة. الأمر نفسه بالنسبة للتخطيط لاستمرارية الأعمال الذي يتطلب دعماً كاملاً من تقنية المعلومات والإدارة العليا. فضلاً عن أن كليهما يعد من المكونات الهامة في العمليات الفعالة لحوكمة تقنية المعلومات.

ملاحظات:

1. Computers at Risk: Safe Computing in the Information Age (Washington, DC: National Academies Press, 1990), http://www.nap.edu/openbook.php?isbn=0309043883.

٢. مختــبرات ضمان المواصفــات (LU) هي منظمة غير ربحية تختــص باختبار واعتماد ســلامة المنتــج. وقد قامت باختبار المنتجات من أجل الســلامة العامــة لأكثر من قرن. www.ul.com/global/eng/pages.

3. Mariane Swanson and Barbara Guttman, Generally Accepted System Security Principles (GASSP), NIST, Version 2.0, June 1996, http://csrc.nist.gov/publications/PubsSPs.html.

٤. معهد التعافي من الكوارث الدولية، مدينة فولز تشيرش، ولاية فرجينيا الأمريكية www.drii.org.

الفصل الحادي عشر

معايير أمن البيانات الخاصة بصناعة بطاقات الدفع (PCI DSS) وقواعد أخرى لحوكمة تقنية المعلومات

يعـد معيار أمن البيانات الخاص بصناعة بطاقـات الدفع Payment Card Industry Data Security Standard PCI DSS أحـد أفضـل الممارسـات الخاصة بأمن المعلومات وكذلك معيار الصناعة المطلوب من قِبل العديد من المؤسسـات التي تتعامل مع معلومات أصحاب البطاقات بالنسبة للبطاقات الرئيسية كالسحب/ الخصم debit، والائتمان credit ، وبطاقات الدفع الآلي ATM والبطاقات المستخدمة في نقاط البيع Point-Of-Sale (POS) الموجـودة في محـلات بيع التجزئة. وقد تـم تعريف هذا المعيار مـن قبل مجلس معايير صناعـة بطاقات الدفع وأمن البيانـات Data Security Standards Council PCI، وقد تـم وضع هذا المعيار لزيادة الضوابط التي تحيـط ببيانات حامل البطاقة وتقليل عمليات الاحتيال على البطاقات الائتمانية، وذلك باسـتخدام مجموعة من أفضل الممارسات المُوصَى بها. ففي ظل الاعتماد على اسـتخدام بطاقات الدفع في مختلف أشـكال الأعمال التجارية في جميع أنحاء العالم هذه الأيام، ينبغي على المؤسسـات التي تستقبل البطاقات الائتمانية لإتمام عملياتها التشـغيلية على مختلف المسـتويات أن تلتزم بمعيـار PCI DSS. إن فهم هـذا المعيار ومتطلبات الامتثال به يعتبر واحد مـن العناصر الهامة الخاصة بحوكمة تقنية المعلومات بالنسبة للعديد من كبار مديري الأعمال هذه الأيام.

يقـدم هذا الفصل معيار أمـن البيانات الخـاص بصناعة بطاقات الدفـع PCI DSS، ويناقـش أيضاً أهدافه الرقابية للمسـاعدة في بناء وصيانة شـبكة آمنـة لتقنية معلومات. وسـنتحدث أيضاً عن متطلبات الامتثال التي تندرج تحت هذه القواعد، وكل من عمليات التقييمات المناسـبة للأمن في المؤسسات الكبيرة إلى جانب عمليات الاستخدام الاختياري أو التطوعي لاستبيانات التقييم الذاتي Self-Assessment Questionnaire (SAQ) المتعلقة بمعيار PCI DSS في الشركات الصغيرة. وتشـتمل قواعد هذا المعيار على ما هو أكثر بكثير

مـــن مجرد المعامـــلات الخاصة بالبطاقات الائتمانية للعملاء، حيـــث يعد الامتثال هنا جزءاً رئيسياً وهاماً في حوكمة تقنية المعلومات.

كـــما يتحدث هذا الفصل أيضاً بشـــكل مختصر عـــن قانونين آخرين مـــن القوانين الأمريكيـــة التي لها تأثير في حوكمـــة تقنية المعلومات وهما: قانـــون غرام ليتش بليلي Gramm-Leach-Bliley (GLBA) الـــذي يغطي العمليات الخاصة بجمع المعلومات الشـــخصية الخاصة بالمستهلكين والإفصاح عنها وحمايتها، بالإضافة إلى مناقشة القواعد الخاصة بحفظ ســـجلات تقنية المعلومات التي تعـــد من عناصر قانون الرعاية الصحية المعـــروف بقانون HIPAA. إن نقاشـــنا الدائر حول كل مـــن GLBA وHIPAA يعد مجرد أمثلة للعديد من القوانين والقواعد التي نواجهها اليوم والتي تشتمل على العديد من قضايا حوكمة تقنية المعلومات.

في الولايـــات المتحدة الأمريكية والاتحاد الأوروبي وغيرها من الأماكن في كل أرجاء العالم، نلاحـــظ أن تلك القوانين، وهذا العدد غير المحدود كما يبدو من القوانين والقواعد والمعايير الأخـــرى التي قد تم إصدارها مؤخراً؛ تحتوي على الأقل على بعض القضايا المتعلقة بحوكمة تقنيـــة المعلومات. وفضـــلاً عن المعلومات الموجودة في ثنايا هـــذا الفصل حول PCI DSS وGLBA وHIPAA، فـــإن الفصـــول الأخـــرى ســـتقوم بتغطية القواعـــد والمعايير المختلفة لحوكمة تقنية المعلومات. على ســـبيل المثال، قدم الفصل الســـابع من هذا الكتاب المعايير الدولية الصادرة عن الآيزو فيما يخص حوكمة تقنية المعلومات، كما سيناقش الفصل السابع عشر من هذا الكتاب الإرشـــادات الخاصة باتفاقيات مســـتوى الخدمـــة لتقنية المعلومات وكذلك الإرشـــادات الخاصة بقيمة تقنية المعلومات Val IT الصادرة عن جمعية ISACA، وكلاهما هام جداً بالنســـبة لحوكمـــة تقنية المعلومات. لذا ينبغـــي دائماً على القائمين على تقنية المعلومات المؤسسية أن يكونوا على الأقل على علم بتلك القوانين والقواعد وغيرها من المعايير الجديدة ومدى تأثيرها في الممارسات الجيدة لحوكمة تقنية المعلومات.

معلومات أساسية عن صناعة بطاقات الدفع وأمن البيانات PCI DSS والمعايير الخاصة بها:

بدايـــةً من مطلع ســـتينيات القرن الماضي، أصبحت بطاقات الائتمان البلاســـتيكية ذات النقوش البارزة من الأدوات الشـــائعة وقتها والتي استُخدمت بشكل أساسي من قبل رجال

الأعمال والمهنيين لشراء تذاكر الطيران، ودفع فاتورة عشاء العمل، وشراء وقود السيارة. ولا تــزال بعض الشركات الأولى في هذا المجال والمُصْدِرة لهــذه البطاقات العامة موجودة حتى الآن، كشركــة أمريكان إكســبريس American Express، في حين أن أنواعاً أخرى لبطاقات الائتــمان كانت تحمل أســماء مثل كارت بلانــش Carte Blanche وداينرز كلوب Diners Club لم يعــد لهــا وجود في الوقت الراهن. وقد تم إصــدار بطاقات أخرى لإحدى شركات الوقــود أو أحد المحلات التجاريــة، وكانت تلك البطاقات مفيدة فقــط في شراء مثل هذه المنتجــات أو في التعامــل مع هؤلاء التجــار. وقد كانت البطاقة الخاصــة بشركة أمريكان أكســبريس رائجة بشــكل بارز نظراً لاســتخدامها لدى العديد من التجار الذين اتفقوا على قبــول التعامل بهــا. إلا أن إصدارها ظل مقتصراً على النخبة الذيــن تتوافر لديهم المعايير الائتمانية الشخصية القوية والمفروضة على إصدار مثل هذا النوع من البطاقات.

في سبعينيات القرن الماضي، ظهرت بطاقات الائتمان فيزا Visa وماستر كارد MasterCard، ومع مطلع الثمانينيات من القرن نفسه ظهرت بطاقة الائتمان ديسكفر Discover. حيث تــم ترخيص وإصدار كل بطاقة من هذه البطاقات عن طريق البنك المحلي الخاص بحاملي هذه البطاقات بحيث تتبع لمجموعة مســتقلة تكون مســؤولة عن إدارة العلامة التجارية الخاصة بالبطاقة ورسوم استخدامها في الأعمال التجارية التي تقبل تلك البطاقة. وقد شاع استخدام تلك البطاقات الائتمانية، بحيث أصبح العديد من المستهلكين هذه الأيام يحملون في جيوبهم عدداً كبيراً من البطاقات التي تصدر من بنوك مختلفة.

ازدهرت البطاقات الائتمانية ونجحت في جميع أنحاء العالم، وقد صاحب ذلك (الازدهار) زيادة مســتوى المخاطر التــي تتعلق بالاحتيال على البطاقات الائتمانيــة وأمنها وحمايتها. وبالرغــم من أن البنك هو المســؤول عن إصدار مثل تلك البطاقات الائتمانية للأشــخاص، فإنه قد تم إنشــاء شركات مســتقلة لإدارة كل علامة من هذه العلامــات التجارية الكبرى الخاصة بتلك البطاقات. فعلى سبيل المثال، تقوم إحدى هذه الشركات بالتعامل مع جميع بطاقــات فيــزا كارد Visa Card، في حين أن هناك شركة أخرى تتعامل مع بطاقات ماســتر كارد MasterCard. أمــا فيما يخص أمــن تلك البطاقات فقد كانت هناك اهتمامات تكاد تكون متشابهة بين تلك الشركات المعنية بإدارة كل بطاقة من هذه البطاقات، وذلك لإيجاد مســتوى إضافي من الحماية بالنســبة للشركات المُصْدِرَة لتلــك البطاقات، وذلك عن طريق

ضمان أن التجار المتعاملين معهم لابد أن يلتزموا على الأقل بالحد الأدنى من مستويات الأمن عند قيامهم بحفظ ومعالجة ونقل البيانات الخاصة بحاملي تلك البطاقات.

ولإيجاد حل لتلك الاختلافات البسـيطة الموجودة بين مختلف أنواع البطاقات الائتمانية على نحو أفضل، فقد تم تشكيل مجلس صناعة بطاقات الدفع Payment Card Industry (PCI) council. وقد كانت قضايا الأمن واختلاف القواعد أحد أبرز المشـكلات المثارة بين جميـع أعضاء المجلـس. وفي عام ٢٠٠٤ قامت شركات البطاقـات الائتمانية بتوحيد جميع السياسـات الفردية لكل منهم، وتشـكيل مجلـس المعايير الأمنيـة Security Standards Council والـذي نتج عنه إطلاق الإصدار الأول من معيار أمن البيانات PCI DSS. وكان عبـارة عن معيار وليـس قانوناً، إلا أنه كان مـن المتوقع أن يلتزم به جميـع التجار الذين يستخدمون بطاقات الائتمان.

وبالنظر إلى كل التغيرات التي جرت على العمليات الخاصة بمعالجة البطاقات الائتمانية في السنوات الأخيرة، من خلال مميزات مثل المعالجة اللاسلكية، والمخاطر الخاصة بالسرقة علاوة على سرقة أرقام البطاقات المرخصة والمخزنة في سـجلات أعمال المؤسسة، وغيرها من مخاطر الاحتيال المتزايدة، لذا فقد مر معيار PCI DSS بعدة مراحل من المراجعات والتنقيحات منذ الإصدار الأول له. وقد يتحقق الالتزام بقواعد المعيار PCI DSS من خلال التقييمات الذاتية الاختيارية أو التطوعية بالنسـبة لصغار مسـتخدمي PCI. إلا أن الامتثـال بها يكون إلزامياً بالنسـبة للشركات الكبيرة التي تقوم بمعالجة تلك البطاقات الائتمانية. وسواء كانت بطاقات الدفع تسخدم هذه الأيام من خلال اختصاصيي تقنية المعلومات أو من خلال أي من عمليات تشغيل المؤسسة، فإنه ينبغي أن يكون لدى مسئولي الأعمال التنفيذيين فهم عام لمعيار PCI DSS ولمدى تأثيرة في العمليات التشغيلية للمؤسسة على الأقل.

يستعرض الشكل التوضيحي (١١-١) المتطلبات ذات المستوى الرفيع الخاصة بمعيار PCI DSS والأهداف الرقابية المرتبطة به. سـنتحدث بتفصيل أكثر في الأقسـام التالية عن الغاية الكامنة وراء متطلبات هذا المعيار، وسنوضح المتطلبات الضرورية للحفاظ على بيانات حامل البطاقة، ثم سنقوم بالحديث عن طبيعة وأهمية عمليات التقييم الذاتي الخاصة بهذا المعيار. وستتناول فصول أخرى مواضيع مهمة جداً لتحقيق الامتثال الفعال لهذا المعيار. على سبيل

المثال، قد ناقش الفصل العاشر من هذا الكتاب القضايا المتعلقة بأمن تقنية المعلومات التي تعد من الأمور الهامة بالنسبة للحوكمة الفعالة لتقنية المعلومات. هذه القضايا نفسها على الدرجة نفسها من الأهمية فيما يتعلق بتحقيق الامتثال لمعيار PCI DSS.

بالإضافة إلى معيار أمن البيانات DSS، فقد قام PCI بإصدار معيارين آخرين لهما علاقة بهذا المعيار وهما:

١- معيار أمن التعاملات الخاصة بالأرقام الشخصية السرية الخاصة ببطاقات الدفع PIN Transaction Security (PCI PTS). وهي مجموعة من المتطلبات الأمنية التي ركزت على إدارة الأجهزة المستخدمة لحماية أرقام التعريف الشخصية Personal Identification Number (PIN) لحاملي البطاقات الإئتمانية والأنشطة الأخرى المتعلقة بمعالجة عملية الدفع، متضمناً متطلبات تصميم وصناعة ونقل الجهاز إلى المنشأة التي ستقوم بتطبيقة.

شكل توضيحي (١١-١)

متطلبات معيار أمن البيانات الخاص بصناعة بطاقات الدفع PCI DSS والأهداف الرقابية المرتبطة به

الأهداف الرقابية	متطلبات المعيار PCI DSS
بناء شبكة آمنة والحفاظ عليها.	١. قم بتنصيب وصيانة بنية الجدران النارية لحماية بيانات حامل البطاقة. ٢. لا تستخدم القيم الافتراضية التي يوفرها المورد لتخصيص كلمات المرور وغيرها من معاملات الأمن في النظام.
حماية بيانات حامل البطاقة.	٣. قم بحماية البيانات المخزنة لحامل البطاقة. ٤. قم بتشفير انتقال البيانات الخاصة بحامل البطاقة عبر الشبكات العامة والمفتوحة.
اتباع برنامج لإدارة نقاط الضعف.	٥. قم باستخدام برمجيات محدثة بشكل منتظم للتخلص من الفيروسات وفحص جميع الأنظمة التي تكون عادة عرضة للبرامج الضارة. ٦. قم بتطوير وصيانة تطبيقات نظم آمنة.

تطبيق إجراءات وتدابير قوية وصارمة لضبط الوصول.	٧. قم بقصر الوصول لبيانات حامل البطاقة فقط على الأعمال التي بحاجة إلى معرفة هذه البيانات. ٨. قم بتخصيص معرف فريد ID خاص لكل شخص يمكنه الوصول للبيانات باستخدام الحاسب. ٩. قم بتقييد الوصول الفعلي لبيانات حامل البطاقة.
مراقبة وفحص الشبكات بشكل منتظم.	١٠. قم بتعقب ورصد كل عمليات الوصول لموارد الشبكة وبيانات حاملي البطاقات.
	١١. قم بفحص نظم وعمليات أمن البيانات بشكل منتظم.
الحفاظ على سياسة أمن المعلومات.	١٢. قم بالحفاظ على السياسة التي تقيّم من خلالها أمن المعلومات.

٢. معيار أمن المعلومات الخاص بتطبيقات الدفع (Payment Application (PA DSS. هذا المعيار يخص مطوري البرمجيات والقائمين على تكامل تطبيقات الدفع والتي تقوم بتخزين أو معالجة أو نقل بيانات حاملي البطاقات كجزء من عملية الترخيص أو الاتفاقيات التي تتم عند القيام ببيع هذه النظم أو توزيعها أو ترخيصها للآخرين.

وعلى الرغم من العلاقة الوطيدة بين هذين المعيارين الجديدين والمعيار PCI DSS، فإننا سنركز في حديثنا في هذا الفصل على معيار أمن البيانات الخاصة بصناعة بطاقات الدفع PCI DSS. والذي يعد من المعايير الهامة لحوكمة تقنية المعلومات في العديد من المؤسسات.

حماية بيانات حاملي البطاقات وبرامج إدارة الثغرات الأمنية:

من السهل نوعاً ما أن يقوم التاجر الصغير بإجراء جميع الترتيبات المصرفية الضرورية لتنفيذ المعاملات التي تتم من خلال بطاقة الفيزا أو بطاقة الماستر كارد أو غيرهما، ثم يقوم بعد ذلك بوضع أجهزة قارئة أو ما يسمى بأجهزة الماسحات الضوئية من أجل قبول تلك البطاقات لإتمام عمليات الدفع الخاصة بالمشتريات. حيث يتم نقل معلومات الشراء الخاصة بالبطاقة إلى معالج خاص ببطاقات الائتمان، ثم يحصل التاجر على ثمن المنتجات التي تم شراؤها. ويتم تحميل فاتورة الشراء على حساب بطاقة الائتمان الخاصة بالمشتري. في هذه العملية الشائعة بكثرة، توجد مخاطرة من أكبر المخاطر الأمنية التي

يتــم تجاهلهــا غالباً، وهي أنه من الممكن أن تتم سرقة رقــم البطاقة الائتمانية إلى جانب البيانات التعريفية الخاصة بالعميل واســتخدامها في أغراض غير مشروعة. نذكر هنا على سبيل المثال إحدى الحوادث التي تم فيها التبليغ عن اختراق ما يزيد عن مائة مليون سجل من الســجلات الخاصة بمعلومات العملاء في الولايــات المتحدة على مدار عامين بدأت من عام ٢٠٠٥ وانتهت في عام ٢٠٠٧ [١]. كما أن الاســتخدام غير المشروع لتلك الأرقام الخاصة بالبطاقات الائتمانية التي تم اختراقها سيعرض كلاً من التجار وشركات البطاقات الائتمانية وأصحــاب البطاقات إلى المخاطر. إن الهدف الرئيسي لمعيــار PCI DSS هو توفير حماية كافيــة لبيانات أصحاب البطاقات المحفوظــة في النظام. قد يعتقد المرء أن النظم الخاصة بمــزودي خدمات البطاقات كبطاقة الفيزا أو الماســتر كارد والبنوك المنتســبة لها ســتكون آمنة (كما تشــترط اللوائح المصرفية)، وأنه مــن المتوقع أيضاً أن يقوم الفرد بحماية بيانات البطاقــة الائتمانية الخاصة به أو بها. على أية حال، جرت العادة أن يقوم أصحاب المحال التجارية بمعالجة العديد من أرقام البطاقات الائتمانية مع مرور الوقت. فالمطلب الرئيسي لمعيار PCI DSS هو ضرورة أن تقوم المؤسسة بتأمين وحماية البيانات الخاصة بالبطاقات الائتمانية.

المشكلة هنا هي أن أصحاب المحال التجارية هم من يقومون في أغلب الأحيان بعمليات تأمين الكثير من البيانات الخاصة بالبطاقات الائتمانية لعملائهم بصورة غير كافية. وفي جزء من الدراسة الكبرى التي جرت عام ٢٠٠٧ عن أصحاب المحال التجارية في الولايات المتحدة الأمريكية والاتحاد الأوروبي، وجدت الشركة الاستشــارية فورســتر[٢] Forrester أن أصحاب المحــال التجارية يقومون عادة بالاحتفاظ بكميات هائلــة من البيانات الخاصة بالبطاقات الائتمانية الخاصة بعملائهم، وتشــتمل هذه البيانات على أرقام البطاقات وتواريخ انتهائها وأســماء وعناوين أصحابها. تحتفظ المؤسســات عادة بمعلومات أكبر بكثير من مجرد أرقام البطاقات الائتمانية، ولاســيما تواريخ انتهاء البطاقات والأســماء والعناوين والرموز الأمنية. وفي ظــل الافتقار إلى التدابير والإجــراءات الأمنية القوية لتقنية المعلومات المؤسســية، قد يؤدي هذا التأمين الضعيف لمعلومات بطاقات الائتمان إلى العديد من الاختراقات والمشاكل الأمنية الجسيمة.

في أغلب الأحيان نجد أنه إما أن تكون عمليات التشــفير والضوابط الأمنية الأخرى ضعيفة أو حتى غير مطبقة. وفي بعض الأحيان يمكن أن تواجة المؤسســات التي تقوم بمعالجة حجم هائل من المعاملات مخاطر ناجمة عن التراخي في عمليات معالجة المسائل الضرورية المتعلقة بالبطاقــات الائتمانية للعمــلاء. وأمثلة على المخاطر والمشــاكل يمكن مشــاهدتها من خلال الأحــداث التي وقعت في شركات تي جا إكس TJX عــام ٢٠٠٣، والتي تمتلك نحو ٢٥٠٠ متجر مــن متاجر التجزئة. فقد تم اختراق نظم الحاســبات الخاصة بها للمرة الأولى بواســطة أحد قراصنــة (Hacker) شــبكة الإنترنت الذي تمكــن من اختراق النظام والوصــول إلى معلومات تتعلق بالتعاملات الخاصة بالبطاقات الائتمانية للعملاء، وقد استمر ذلك لعدة شهور إلى أن تم اكتشاف أمره في عام ٢٠٠٦ [٣]. وقد اشتملت تلك المعلومات على أسماء العملاء وأرقام بطاقات الائتمان الخاصة بنحو ٤٥,٧ مليون بطاقة ســحب وائتمان تم سرقتها من خلال معاملات تمت خلال الفترة من شهر يناير إلى شهر نوفمبر من السنة نفسها. فقد ضاعت خصوصية بطاقات الائتمان لدى العديد من العملاء، وتعرضت شركة TJX لخسائر هائلة سواء كانت على الصعيد المادي جراء دعاوى التسوية القضائية أو على الصعيد الخاص بسمعتها.

إن تلــك الواقعة الخاصة بــشركات TJX ما هي إلا أحد الأمثلة على المخاطر التي يمكن أن تتعرض لها المؤسسة في حال كانت الضوابط الخاصة ببطاقة الائتمان لديها ضعيفة. ومن المؤكد أن يُظْهِــر لنا تحليل الأحداث الخاصة بمثل هذه الاختراقات الأمنية مجموعة من نقاط الضعف الأمنيةِ الشائعة التي يتم معالجتها الآن من خلال معيار PCI DSS. فقد تم تصميم نوع خاص مــن الضوابط الأمنية لتقنية المعلومات، وهو معيار PCI DSS والذي يشــتمل على متطلبات تفصيليــة، تحديداً، لهذا النوع من المخاطر - لتقليل فرص التعرض لإفشــاء (تسريب) أو سرقة البيانات وكذلك تقليل التأثير الناتج جراء هذه السرقة أو إفشاء البيانات في حال وقوعه. تُظْهِر التحقيقات التي تتم بشــكل مستمر بعد هذه التعرضات للمخاطر الخاصة بإفشاء البيانات أَو سرقتها، بعض وليس كل الانتهاكات الشائعة الخاصة بمعيار PCI DSS وهي:

- ضوابط غير كافية على عملية الوصول للبيانات، وذلك من خلال التركيب غير الســليم من قِبل أصحاب المحال التجارية لنظم نقاط البيع POS، الأمر الذي يســمح للمســتخدمين الأشرار من الوصول إلى المسارات التي تستهدف موردي نقاط البيع POS.

• الافتقار إلى التقنيات الخاصة بعمليات التسجيل أو المتابعة، مثل النظم الخاصة بمراجعات السجلات والكشف عن التسللات ومنعها، والنظم المساعدة في إجراء المسوحات الربع السنوية لنقاط الضعف، والنظم المسؤولة عن متابعة سلامة الملفات.

• تخزين بيانات الشريحة الممغنطة لبطاقات الائتمان. فالعديد من الكيانات التي تم إفشاء بياناتها لا يعلمون أن الأنظمة التي لديهم تقوم بحفظ مثل تلك المعلومات، مما يوفر كمية هائلة من المعلومات للمتسللين.

• عدم تغيير الإعدادات وكلمات المرور الافتراضية عند تركيب النظام. هذا بالإضافة إلى عدم إزالة الخدمات غير الضرورية وغير الآمنة أو تأمينها أثناء تثبيت النظام.

• تطبيقات الويب سيئة التشفير تؤدي إلى نقاط ضعف قد تسمح بالوصول إلى قاعدة البيانات التي تحتفظ ببيانات أصحاب البطاقات من إحدى مواقع الإنترنت بشكل مباشر.

• التطبيق السيئ للضوابط الخاصة بالتطبيقات الشبكية، الأمر الذي يعرض البيئة الخاصة ببيانات أصحاب البطاقات عن غير دراية إلى نقاط الضعف الموجودة في أجزاء أخرى من الشبكة التي لم يتم تأمينها بعد، كنقاط الاتصال اللاسلكية غير المؤمنة والثغرات الناجمة عن استخدام الإيميل وتصفح الإنترنت.

لسنا هنا بصدد تقديم درس تعليمي حول القضايا الأمنية الخاصة بتقنية المعلومات، وإنما بصدد تأكيد أن أمن تقنية المعلومات هو أحد العناصر الهامة في حوكمة تقنية المعلومات، وأنه أيضاً أحد العناصر الحساسة في المعاملات المتعلقة بالبطاقات الائتمانية. إذ يستطيع المدير الأول (الأعلى) الاستعانة بالنقاط السابقة ليقوم بتوجيه أسئلة تتعلق بأمن وسلامة العمليات التشغيلية في المؤسسة فيما يخص البطاقات الإئتمانية. على كل حال، بما أن معظم معلومات بطاقات الائتمان يتم نقلها مباشرة من نقاط البيع حيث المكان الذي يتم فيه إتمام عمليات البيع عن طريق بطاقات الائتمان، فالقاعدة الأساسية التي يجب التأكيد عليها بالنسبة لأصحاب المحال التجارية هي عدم نقل تلك البيانات الخاصة بالبطاقات الائتمانية للعملاء داخلياً على الإطلاق.

متطلبات معيار PCI DSS:

يجب على المؤسسة اتباع الخطوات اللازمة لتحقيق الامتثال لمعيار PCI DSS، وذلك من خلال تضافر الجهود بين كل من العاملين في تقنية المعلومات، والتدقيق الداخلي، والقانونيين، والعاملين بالائتمان والشئون المالية. وقد تم تلخيص هذه الخطوات في الشكل التوضيحي (١١-١) حيث سيكون لهذا المعيار المتطلبات التالية:

- **بناء شبكة آمنة والحفاظ عليها:** تحدث الفصل العاشر من هذا الكتاب عن أهمية أمن تقنية المعلومات في المؤسسة. إلا أن قواعد معيار PCI DSS تشترط أمرين محددين هنا: الأول، هو أنه يجب على المؤسسة أن تقوم ببناء وتركيب إعدادات الجدران النارية على نظم تقنية المعلومات لديها وصيانتها، وذلك لحماية بيانات حاملي البطاقات الائتمانية. ويعد مفهوم الجدران النارية من المفاهيم الشائعة بين العاملين في مجال أمن تقنية المعلومات، غير أن هذا الأمر قد لا يكون شائعاً لدى المسئول التنفيذي للأعمال. يمكننا النظر إلى الجدران النارية لتقنية المعلومات على أنها تشبه أبواب الخروج ذات الاتجاه الواحد الموجودة في معظم المسارح. حيث يستطيع الشخص المرور من خلال تلك الأبواب إلى الخارج في حال اندلاع حريق، ولا يستطيع أحد موجود في الخارج من استخدام تلك الأبواب للدخول. وبالرغم من أن الضوابط الخاصة بالجدران النارية أصبحت اليوم شائعة الاستخدام في العديد من بيئات أمن تقنية المعلومات، فإنه يتعين على المؤسسة التأكد من أنه قد تم تركيب وإعداد تلك الجدران النارية على عناصر نظم تقنية المعلومات لديها والتي تشمل البيانات الخاصة بالبطاقات الائتمانية.

بالإضافة إلى ذلك، لا يجب على المؤسسة أن تستخدم الإعدادات الافتراضية المقدمة من قبل المورد والخاصة بكل من كلمات المرور Passwords وغيرها من المعاملات والمحددات الأمنية الأخرى التي يقوم المورد بتقديمها. وهي ببساطة تعتبر من الممارسات الأمنية الجيدة التي يتم تجاهلها غالباً. فقد تطلب البرمجيات التي يتم توفيرها من قبل المورد من العملاء الجدد إدخال "١٢٣٤" كلمة مرور أولية عند الإعداد الأوليّ للتطبيق، ومن ثم تغييرها بمجرد تركيب التطبيق. وهناك العديد من المستخدمين الذين لا يُحَمِّلون أنفسهم عناء تغيير كلمة المرور، وهو الأمر الذي يجعل النظام دائماً عرضة للاختراقات من قبل المتطفلين الساعين للوصول إلى البيانات.

• **حمايــة البيانات الخاصة بحاملي البطاقات الإئتمانية:** هناك العديد من الضوابط الأمنية لتقنية المعلومات التي تندرج تحت هذا المطلب متضمناً ذلك، عمل نســخ احتياطية من البيانات لاســترجاعها عند الحاجة، وتشــفير البيانات أثناء تخزينها ونقلها، وحفظ كل ما يتعلق بوســائط تقنية المعلومات الخاصة بأصحاب البطاقات الائتمانية في مواقع حقيقية مؤمنــة. وتعد هذه الإجــراءات الخاصة بحماية بيانات حامــلي البطاقات الائتمانية من المطالب الهامة لحوكمة تقنية المعلومات.

• **اتبــاع برنامــج يقوم بإدارة الثغــرات أو نقاط الضعف:** تحدث الفصــل الثامن من هذا الكتــاب عن إدارة المخاطر الخاصــة بتقنية المعلومات. وكان يجب أن يكون هناك تركيز بشكل خاص على التقنيات الخاصة بإدارة المخاطر وتقدير نقاط الضعف والثغرات الأمنية بالنســبة للبيانات الخاصة بالبطاقات الائتمانية المخزنــة أو التي يتم معالجتها من خلال موقع المؤسســة. كما ينبغي أيضاً أن يقوم قســم تقنية المعلومات في المؤسسة باستخدام برامج محدثة بشكل دوري ضد الفيروسات للتنبؤ بالبرامج الضارة.

• **تطبيــق إجراءات وتدابير قويــة وصارمة لضبط الوصول للبيانات:** تعد العمليات القوية لأمن تقنية المعلومات من الأمور الضرورية لتحقيق هذا المطلب. حيث تُســتخدم بعض التقنيات الرقابية الرئيسية لتحقيق ما يلي:

o فرض القيود على عمليات الوصول الحقيقية لبيانات أصحاب البطاقات الائتمانية.

o اقتصــار عمليات الوصول إلى بيانات أصحاب البطاقات فقط على الأعمال التي تحتاج إلى تلك البيانات فعلاً.

o تخصيص معرف فريد Unique ID لكل شخص يصل إلى البيانات عبر الحاسب الآلي.

هذه هي بعض الضوابط الرئيسية الخاصة بعملية الوصول إلى تقنية المعلومات. ويمكن لمســئولي الأعمال التنفيذيين أن يطلبوا من الموظفين المســؤولين عــن أمن تقنية المعلومات تقديم شرح تفصيلي عن التقنيات المستخدمة لضبط عمليات الوصول إلى تقنية المعلومات في المؤسســة. وعلى الرغم من أن هناك العديد من المصادر المطبوعة وكذلك المنشورة على شــبكة الويب بشــأن معلومات حول الضوابط الخاصة بالوصول وأمــن تقنية المعلومات،

فـإن مؤلف هذا الكتاب قد قام بوضع كتاب آخر[٤] حول تلك الموضوعات الموجهة لمدققي تقنية المعلومات، غير أنها قد تزود مسئولي الأعمال التنفيذيين ببعض الملخصات الجيدة عن المعلومات الأساسية لأمن تقنية المعلومات.

• **مراقبة وفحص الشـبكات بشكل منتظم:** يجب على المؤسسة تعقب ومراقبة جميع عمليـات ومحـاولات الوصول إلى موارد الشـبكة وبيانـات أصحاب البطاقـات الائتمانية. فبالإضافة إلى الشرط أو المطلب الخاص بالرقابة والتتبع، فإن معيار PCI DSS يشترط أيضاً أن تقوم المؤسسة بفحص النظم والعمليات الأمنية الخاصة بها بصورة منتظمة. وتكون هذه المهمة غالباً من مسـؤولية وحدة التدقيق الداخلي ومدققي تقنية المعلومات المتخصصين. وسـنناقش بمزيد بالتفصيل في الفصل التاسع عشر من هذا الكتاب قضايا التدقيق الداخلي الخاصة بحوكمة تقنية المعلومات.

• **اتباع سياسـة لأمـن المعلومات:** تدعو هذه السياسـة الأخيرة الخاصـة بمعيار PCI DSS المؤسسـات إلى اتباع السياسات التي تعالج قضايا أمن المعلومات. وهذا مشابه جداً للعمليات الأخرى لحوكمـة تقنية المعلومات التي تم الحديث عنها في العديد من الفصول المختلفة لهذا الكتاب. وتعد هذه السياسـات من الأمور الهامة بالنسبة للمؤسسة للتعرف على أفضل الممارسـات التي من الضروري تطبيقها، غـير أنه من الضروري أيضاً إيصال تلك السياسات لجميع أصحاب المصالح لتكون قواعد عامة يجب اتباعها.

تعـد الشروط أو المتطلبات الخاصة بمعيار PCI DSS التي تم ذكرها أعلاه أكثر تحديداً من الإرشـادات العامة التي سـيتم تناولها في هذا القسـم. إذ إن أكثر مديري الإدارة العليا سـيبحثون عن المعايير رفيعة المسـتوى. في حين سـيبحث أخصائي أمن الحاسبات في تقنية المعلومات عن متطلبات أكثر تفصيلاً. على سبيل المثال، يحتوي الشكل التوضيحي (١١-٢) على الإرشادات الخاصة بمعيار أمن البيانات DSS لواحد من هذه المتطلبات. فهذه المعايير تكون على مسـتوى مدقق تقنية المعلومات الماهـر أو المتخصص في أمن تقنية المعلومات. النقطة الرئيسـية هنا هي أنه يجب على المؤسسـة إيجاد بعض الإجراءات الرقابية القوية للمحافظة على الامتثال لقواعد معيار PCI DSS.

بالنسبة للمؤسسات المتوسطة والكبيرة التي مع الوقت قد اكتسبت الخبرة في بناء وتشغيل نظم تقنية المعلومات الخاصة بها، فقد تبدو تلك المتطلبات الخاصة بقواعد معيار PCI DSS أكثر قليلاً من الممارسات الجيدة للرقابة الداخلية والشائع استخدامها والتي تعتبر بمثابة متطلبات رئيسية لتحقيق الإمتثال لقانون SOx كما وضحنا في الفصل الثاني من هذا الكتاب. في جميع الأحوال فإن الاختلاف الرئيسي هنا هو أن المؤسسة لن تخضع أبداً لعملية التدقيق الخارجي اللازمة للتصديق على مستوى امتثالها لمعيار PCI DSS. وإنما تدعو المعايير في هذه الحالة معظم المؤسسات التي تمارس القليل من نشاط البطاقات الائتمانية للقيام بمراجعة وتأسيس امتثالها لمعيار PCI DSS، وذلك من خلال عملية التدقيق والتقييم الذاتي.

شكل توضيحي (١١-٢)

المتطلبات الخاصة بتتبع ومراقبة الوصول إلى موارد الشبكة وبيانات أصحاب البطاقات

١. وضع عملية لربط جميع العمليات التي يقوم بها كل مستخدم للوصول إلى مكونات النظام، خاصة تلك العمليات التي تتم من خلال الامتيازات الإدارية.
٢. تطبيق الرقابة الآلية للمسارات على جميع مكونات النظام لإعادة بناء الأحداث التالية: - جميع العمليات الفردية التي يقوم بها المستخدم للوصول إلى بيانات أصحاب البطاقات. - جميع الإجراءات التي ينفذها المستخدمون أصحاب الامتيازات الإدارية أو الأصلية. - الوصول إلى جميع مسارات التدقيق. - محاولات الوصول المنطقية غير السليمة. - استخدام تقنيات التعريف والتوثيق. - تهيئة سجلات التدقيق. - إنشاء وحذف كائنات على مستوى النظام.
٣. القيام بتسجيل المدخلات ومسارات التدقيق المتعلقة بكل حدث من الأحداث التي تمت على جميع مكونات النظام، والتي تشتمل على الأقل على هوية المستخدم ونوع الحدث والوقت والتاريخ ومؤشر نجاح أو فشل الحدث وبداية الحدث وهوية كل من البيانات أو مكون النظام أو المورد الذي تأثر بهذا الحدث.

٤. باســتخدام تقنية المزامنة، قم بمزامنة جميع الســاعات والأوقات الحاسمة في النظام وقم بتطبيق ضوابط للحصول على الوقت وتوزيعه وحفظه.
٥. تأمين مسارات التدقيق بحيث لا يُسمح بتعديلها.
٦. مراجعة السجلات الخاصة بجميع مكونات النظام المتعلقة بالمهام الأمنية مرة في اليوم على الأقل.
٧. الاحتفاظ بتاريخ مسارات التدقيق لمدة عام واحد على الأقل، ولا بد أن يكون هناك سجلات لثلاثة أشهر على الأقل من التاريخ الحالي متاحة أو متوفرة للتحليل.

عملية التقييم الذاتي لمعيار PCI DSS:

لــكي تتأكد المؤسســة من امتثالهــا أو اتباعها لــبعض المتطلبات الخاصــة بأحد المعايير، فمن الطبيعي ومن الضروري أيضاً الاســتعانة بطــرف خارجي لفحص هذا الامتثال والتأكد من مدى تطبيقه. على ســبيل المثال، من الضروري أن يقوم المدققون الخارجيون (مكاتب التدقيــق الخارجي) - مكاتب المحاســبة القانونية في الولايــات المتحدة الأمريكية؛ بمراجعة القوائــم المالية الخاصة بالمؤسســة والتصديق على مدى صحتها. ومــن الضروري أيضاً أن يكون هناك مراجعون متخصصون مســتقلون يقومون بمســاعدة المؤسسة على التأكد من مدى امتثالها لأي معيار من معايير الأيزو متضمنة تلك التي تحدثنا عنها في الفصل الســابع من هذا الكتاب. ولكن نظراً لوجود عدد كبير من المحال التجارية – الصغيرة نسبياً غالباً – التي تتعامل مع بيانات البطاقات الإئتمانية، ونظراً لأن تكلفة الاستعانة بمراجعين خارجيين ســتكون مرتفعة بعض الشيء؛ فقد سمحت منظمة المعايير الخاصة بصناعة بطاقات الدفع للمؤسسات بالقيام بتنفيذ نشاط التقييم الذاتي للتحقق من امتثالها للمعايير الصناعية.

إن اســتبيان أو اســتطلاع التقييم الذاتي Self-Assessment Questionnaire (SAQ) الخــاص بمعيــار PCI DSS ما هو إلا أحد الأدوات المســتخدمة لمســاعدة أصحاب المحال التجارية ومقدمي الخدمات على القيام بعملية تقييم ذاتي لمعرفة مدى التزامهم وامتثالهم لمعيــار PCI DSS. ويمكننــا إيجاد العديد من النســخ التفصيلية الخاصــة بمعايير التقييم الذاتي من خلال زيارة الموقع www.pcisecuritystandards.org/security_standards/index.php. حيث تدعو تلك المعايير الخاصة بالتقييم الذاتي إلى ما يلي:

- بنـاءً على التوجيه الخـاص بمجلس المعايير الأمنية الخاصة بصناعـة بطاقات الدفع PCI حول "اختيار استبانة التقييم الذاتي والتصديق على أفضل تطبيق لها على المنظمة الخاصة بك". فإنه يجب على المؤسسـة اختيار استبانة التقييم الذاتي المناسبة لمقدمي الخدمات وأصحاب المحال التجارية لديها.
- بعد اكتمال الاسـتبانة المناسـبة للتقييم الذاتي SAQ بنجاح، تستطيع المؤسسة التصديق على شـهادة ذاتية تدل على أنها مؤهلة لتنفيذ (بل وأنها نفذت) بالفعل نشـاط التقييم الذاتي الخاص بالامتثال لمعيار PCI DSS.

طبقاً لمتطلبات المعايير الصناعية فإنه ينبغي على جميع المستخدمين الرئيسيين للبطاقات الائتمانية الاسـتعانة بمُقَيّم مسـتقل للقيام بمراجعة هذا الامتثال، وهذا مشابه للمراجعات الخاصـة بالامتثال بمعايير المنظمة الدولية للمواصفـات والمعايير ISO التي تحدثنا عنها في الفصل السـابع من هذا الكتاب. حتى بالنسـبة للمؤسسـات الأصغر حجماً، فإن الامتثال بمعايير أمن المعلومات ممكن أن يعود بالنفع والفائدة على أعمالها، في حين أن عدم الامتثال بهـا قد يـؤدي إلى عواقب وخيمة وخطيرة طويلة الأجـل. إن الامتثال بقواعد معيار PCI DSS هام للأسباب التالية:

- الامتثال لمعيار PCI DSS يعني أن النظم آمنة، وأنه يمكن للمستخدمين الوثوق بالمؤسسة فيما يتعلق بالمعلومات الحساسة الموجودة في بطاقاتهم الائتمانية.
- الامتثال يحسـن من سـمعة ومكانة المؤسسـة لدى المشـترين وشركات المدفوعات من أصحاب العلامات التجارية – الشركاء الذين تحتاج إليهم للقيام بالأعمال التجارية.

الامتثـال هو عملية مسـتمرة ودائمة، ولا يمكن أن تكون عبـارة عن عملية تحدث لمرة واحدة فقط. ويساعد الامتثال في منع المخالفات أو الاختراقات الأمنية الحالية والمستقبلية، كـما يمنع سرقـة بيانات بطاقـات الدفع. ونظراً لأن عمليات إفشـاء (تسريـب) البيانات أصبحـت الآن متطـورة أكثر من أي وقت مضى، نـرى أن مجلس المعايـير الأمنية الخاصة بصناعة بطاقات الدفع PCI يعمل دائماً على مراقبة التهديدات وتحسين الوسائل الصناعية المسـتخدمة للتعامل معها، وذلك من خلال إجراء التحسـينات على المعايير الأمنية الخاصة بصناعة بطاقات الدفع وإجراء التدريبات اللازمة للمختصين في المجال الأمني.

كم أن للامتثال فوائد غير مباشرة، فقد يساعد المؤسسة على أن تكون في وضع أفضل فيما يخص امتثالها بلوائح تنظيمية أخرى مثل قانون إخضاع التأمين الصحي لقابلية النقل والمحاسبة Health Insurance Portability and Accountability Act (HIPAA) الذي سنتحدث عنه لاحقاً في هذا الفصل، وأيضاً كالامتثال لقانون ساربينز أوكسلي SOx الذي تطرقنا إليه في الفصل الثاني من هذا الكتاب. بعبارة أخرى، يمكن أن نقول إن هذا التقييم الذاتي قد يوفر القاعدة الأساسية للإستراتيجية الأمنية للشركة، وقد يحدد أساليب لتحسين فاعلية البنية التحتية لتقنية المعلومات.

قانون جرام ليتش بليلي (GRAMM-LEACH-BLILEY) في القواعد الخاصة بحوكمة تقنية المعلومات:

في أواخر تسعينيات القرن الماضي أقر مجلس النواب الأمريكي قانوناً لتغيير بعض القواعد المعمول بها في المؤسسات المالية القائمة منذ الكساد العظيم الذي حدث في ثلاثينيات القرن الماضي. وقد عُرِف هذا القانون الجديد رسمياً باسم قانون تحديث القطاع المالي لسنة ١٩٩٩، والذي اشتهر أكثر باسم قانون جرام ليتش بليلي (Gramm Leach Bliley Act GLBA). هذا القانون عبارة عن مجموعة من المتطلبات المتعلقة بالخصوصية والهادفة لحماية المعلومات المالية الشخصية الخاصة بعملاء المؤسسات المالية. ويتكون هذا القانون التشريعي المتعلق بالخصوصية من ثلاثة أجزاء رئيسية هي: (١) قاعدة الخصوصية المالية و(٢) قاعدة الحماية و(٣) ما يعرف باسم "أحكام التحجج الاحتيالى" (استخدام الأكاذيب للوصول لبيانات الآخرين) Pretexting provisions. بينما لم يسمع المهنيون قط بمفهوم "التحجج الاحتيالى" الذي جاء به هذا القانون، فإنه سيتم مناقشة هذا المفهوم واعتباراته الخاصة بحوكمة تقنية المعلومات الموجودة في مواد أخرى من هذا القانون في الأجزاء اللاحقة. يمنح هذا القانون GLBA السلطة إلى ثماني وكالات وولايات اتحادية أمريكية رسمية مختلفة للقيام بإدارته، كما يفرض هذا القانون أيضاً مجموعة جديدة من القواعد المتعلقة بالخصوصية التي يتم تطبيقها على المؤسسات المعروفة عموماً باسم "المؤسسات المالية". ولا نعني بهذه المؤسسات البنوك، وشركات التورق، وشركات التأمين التقليدية فحسب، ولكن نعني أيضاً المؤسسات التي تقدم لعملائها أنواعاً مختلفة من المنتجات

والخدمـات المالية كخدمات الإقراض، والوسـاطة، ومختلف أنواع القروض الاسـتهلاكية، وخدمـات نقل وحماية الأمـوال، وخدمات إعداد الإقرارات الضريبيـة الفردية، وخدمات تقديـم النصائح المالية والاستشـارات الائتمانية، وخدمات التأسـيس العقاري السـكني، وخدمـات تحصيـل القروض الاسـتهلاكية وغيرها من الخدمات الماليـة الأخرى. وفي ظل قانون GLBA فإن لجنة التجارة الاتحادية أو الفيدرالية (Federal Trade Commission FTC) هي التي تقوم الآن بالإشراف على تلك "المؤسسات المالية " غير التلقيدية، سواء كان ذلك بشكل مباشر أو من خلال الوكالات الرسمية والاتحادية.

وعلى الرغم من أن المدير الأول الذي يعمل لصالح أحد البنوك أو شركات التأمين في الوقت الراهن قد يكون هو المعني بهذا القانون وبأحكام الخصوصية التابعة له، إلا أنه يمكن اعتباره القاعدة التي تسـتطيع التأثير في العديد من المؤسسات الأخرى، وذلك بسبب المعنى الواسع للمصطلح المعروف "بالمؤسسات المالية". وقد تم تطبيق قواعد هذا القانون على العديد من المؤسسات المالية الخاضعة للوائح الرسمية. على سبيل المثال، قد تم تنظيم شركات التأمين في الولايات المتحدة على أسـاس كل ولاية على حدة، وذلك من خلال الجمعيَّة الوطنيَّة لمُفوضي التأمين National Association of Insurance Commissioners (NAIC)، والتي تعمل بصفـة مجموعة مركزية لتنسـيق ووضع المعايير لتلك اللجـان المعتمدة في الولاية. وأن هذا التحالـف أو المجموعـة NAIC هي التي تفرض قواعد التفويـض الاتحادية لقانون GLBA على شركات التأمين المستقلة التابعة لها والمنظمة من قِبل الولاية الموجودة فيها. وهذا مثال آخـر يوضح كيف تنتقل اللوائح القانونية الاتحادية في الولايات المتحدة في بعض الأحيان من سـلطة الدولة الأمريكية كهيئة الأوراق المالية والبورصة الأمريكية SEC، المعنية بأمور قانون SOx، إلى قواعـد على مسـتوى قوانين الولاية الواحدة، هذا إلى جانـب بعض القواعد المالية العالمية المشابهة. فنحن ننسى غالباً أن بعض اللوائح القانونية للشركات والعديد من المبادئ التشريعية الأخرى في الولايات المتحدة تكون فعالة طبقاً لكل ولاية على حدة. فعلى سـبيل المثـال، يتـم إصدار رخص قائدي المركبات من قبل كل ولاية عـلى حدة. وبالمثل، فإنه وعلى الرغم من أن إدارة الاختبارات الخاصة بالحصول على شهادة محاسب قانوني CPA تتم محلياً من قبل الجمعية الأمريكية للمحاسبين القانونيين AICPA، إلا أن رُخَص المحاسبين القانونيين CPAs يتـم منحها تبعاً لكل ولاية عن طريق مجلس المحاسـبة الخاص بالولاية. فمن خلال

ســلطة الجمعية الوطنية لمفوضي التأمين، وهو الكيان المعني بتنسيق القواعد داخل الولاية، فقــد تم تبني واعتماد قواعد قانــون GLBA من قبل معظم الولايــات في الولايات المتحدة الأمريكية.

قواعد الخصوصية المالية لقانون GLBA:

يواجه المســتخدمون غالباً هذه الأيــام داخل الولايات المتحدة قانــون GLBA وقواعد الخصوصية المالية الخاصة به عند اســتلامهم إشــعارات مفيدة مــن مقدم خدمة البطاقات الائتمانية تصف لهم قواعد الخصوصية الخاصة ببطاقاتهم الائتمانية. حيث تشــترط قواعد الخصوصية المالية لقانون GLBA من المؤسســات المالية أن تقوم بتزويد عملائها بإشعارات وملاحظات حــول الخصوصية المالية المتبعة لديهم والتي توضح لهم الممارســات المتبعة في المؤسسة المالية لجمع وتبادل البيانات. ويجب أن يكون إشعار الخصوصية هذا واضحاً جداً وبارزاً وبه إفصاح دقيق عن ممارســات الخصوصية المتبعة في الشركة. كما يجب أن يحتوي هذا الإشــعار عــلى معلومات قامت الشركــة بجمعها عن عملائها وكذلك من المســتهلكين، وأيضــاً معلومات تتعلــق بالجهات التي تتبادل معها الشركــة المعلومات الخاصة بالبطاقات الائتمانيــة، ومعلومات عن الكيفية التي تقوم بها الشركــة بحماية وصيانة هذه المعلومات. يطبق الإشــعار على "المعلومات الخاصة الشخصية" للمســتهلكين والعملاء التابعين للشركة والتــي تقوم الشركة بجمعها والإفصاح عنها، إلا أنه على الصعيد العملي يمكن أن يطبق على معظم أو كل بيانات العملاء الموجودة لدى الشركة. على سبيل المثال، المعلومات الشخصية الخاصــة قــد تكون المعلومات التــي يقوم المســتهلك أو العميل بإدخالها أثناء اســتخدامه لتطبيقــات العقود الائتمانية أو عقود البيع، أو معلومات تتعلق بشــخص ما يمكن الحصول عليها من مصدر آخر كالمكاتب الائتمانية، أو معلومات عن العمليات التي تتم بين الشخص والشركة كالمعلومة التي تتعلق بالرصيد الموجود في الحساب مثلاً. في الحقيقة واعتماداً على قانون GLBA يتم تصنيف المعلومات الخاصة بأي شــخص يُدرج اســمه في قائمة العملاء أو المســتهلكين التابعين لمؤسســة مالية محددة على أنها معلومات خاصة شخصية. ولا تخضع المعلومات التي تعتقد المؤسسة لسبب ما بأنها معلومات عامة قانونياً لقانون GLBA، مثل معلومات قروض الرهن العقاري في الجهة القضائية التي يتم تسجيلها علناً.

وبناء على قانون GLBA فإنه يجب أن تحتوي إشعارات الخصوصية على المعلومات التالية:

- أنواع المعلومات الخاصة الشخصية للعملاء التي تقوم المؤسسة بجمعها.
- أنواع المعلومات الخاصة الشخصية للعملاء التي ستقوم المؤسسة بالإفصاح عنها للآخرين.
- الأطراف التي ستبيح لها المؤسسة الاطلاع على هذه المعلومات، من غير الأطراف الخاضعة للحظر في عدم الإفصاح عن المعلومات.
- أحقية العميل أو المستخدم بالاعتراض على الإشعار ووجود قواعد توضيحية بسيطة عن آلية رفع تلك الاعتراضات.
- السياسات المتبعة في المؤسسة بخصوص مشاركة بيانات شخص لم يعد الآن من أحد عملائها أو زبائنها.
- الإجراءات المتبعة في المؤسسة لحماية خصوصية وأمن المعلومات الخاصة الشخصية لزبائنها وعملائها.

لا يكترث الكثير من المستهلكين هذه الأيام بتلك الإشعارات، على الرغم من أنها يمكن أن تصرح عن رغبة الشركة المالكة للبيانات الخاصة بحسابات العملاء بالقيام بمشاركة اسم العميل مع الآخرين. فبدلاً من هذه الممارسة المستخدمة كثيراً من المستهلكين، والتي هي إتلاف وإهمال الإشعارات أو الملاحظات، فإن قانون GLBA يعطي الحق للمستهلك بأن يقوم بالاعتراض على قيام الشركة بمشاركة تلك المعلومات الخاصة به مع الأطراف الأخرى. ويجب أن يوضح الإشعار - وغالباً بطريقة معقولة ومنطقية - الطريقة التي يمكن اتباعها من قبل المستهلكين لتقديم اعتراضاتهم. على سبيل المثال، طريقة توفير رقم هاتف مجاني للاعتراضات والشكاوى أو توفير نموذج منفصل يحتوي على العنوان تعتبر من الطرق المعقولة للاعتراض بالنسبة للمستهلكين والعملاء، أما مطالبة الأشخاص بأن يقوموا بكتابة رسالة اعتراضية كوسيلة وحيدة لتقديم اعتراضاتهم لا تعتبر أبداً طريقة معقولة ومقبولة. كما يجب أن يوضح إشعار الخصوصية أيضاً أن للمستهلكين الحق (أن يقولوا لا) بالنسبة للسماح بمشاركة معلومات محددة تخصهم. مثل مشاركة معلومات تقرير أو تطبيق ائتماني مع الأقسام أو الفروع المستقلة عن المؤسسة المالية.

يضع قانون GLBA بعض القيود على الكيفية التي يمكن من خلالها لأي شخص يستقبل معلومات شخصية خاصة من إحدى المؤسسات المالية أن يقوم باستخدام تلك المعلومات أو إعادة الإفصاح عنها. فإذا قام المُقْرِض بالإفصاح عن معلومات العميل لمزود الخدمة المسؤول عن بيانات الحسابات البريدية - حيث لا يحق للعميل الاعتراض على ذلك - فإنه ينبغي على مزود الخدمة هذا أن يقوم باستخدام تلك البيانات لأهداف محددة فقط - كإرسال بيانات الحسابات البريدية - ولا ينبغي عليه بيع أو استخدام هذه البيانات لأغراض تسويقية.

إن مبدأ الخصوصية المالية الخاص بقانون GLBA سيكون أكثر تعقيداً عندما نخوض أكثر في أمور تفصيلية تابعة له. في جميع الأحوال، نحن لا نهدف هنا إلى عرض هذا الشرح التفصيلي المتعلق بتلك الجزئية من قانون GLBA، وإنما هدفنا هو فقط توضيح هذه القواعد المتعلقة بالخصوصية وتأثيراتها في حوكمة تقنية المعلومات بشكل عام. لذا يجب على مديري المؤسسات إدراك أن كل المعلومات الشخصية الخاصة تعد معلومات سرية للغاية ولا يمكن القيام ببيعها أو نشرها دون مبرر. وأن للمستهلكين أن يعترضوا وأن يقولوا لا، ويجب على المؤسسة الاحتفاظ بشكل ملائم بتلك السجلات الخاصة بالاعتراضات المقدمة، وأن يتم احترام حقوق المستهلكين في الخصوصية. وينطبق الأمر نفسه على أي مؤسسة تقدم تسهيلات منح ائتمانية ودفع فواتير خاصة بالمستهلكين. وتُعَرِّض المؤسسة نفسها للمخاطر عندما تتعامل مع مبدأ الخصوصية الخاص بقانون GLBA كما لو كان عبارة عن أمر بسيط أو تافه أو إلى حد ما هام، فعدم الالتزام والإخلاص في التعامل مع أي من طلبات الاعتراضات المقدمة، أو البيع غير الصحيح للقائمة البريدية، قد يعرض المؤسسة إلى رفع بعض أنواع الدعاوى القضائية جراء الأضرار الناجمة عن عدم الالتزام بمبدأ الخصوصية الخاص بهذا القانون.

قاعدة الحماية في قانون GLBA:

إن قاعدة الأساليب الوقائية لقانون GLBA تطلب من المؤسسات المالية بأن يكون لديها خطة أمنية معمول بها لحماية خصوصية وسلامة المعلومات الشخصية للعملاء. فعندما يقوم العملاء بفتح حسابات جديدة، أو يقوموا بإجراء عمليات شراء منتجات، فإنهم يفصحون عن بعض معلوماتهم الشخصية، كالعنوان ورقم الهاتف أو رقم بطاقة

الائتمان كجزء من إجراء المعاملات الخاصة بالتطبيق. لذا يجب أن يكون لدى المؤسسة خطة أمنية معمول بها لحماية سرية وسلامة هذه البيانات الشخصية التي قام المستهلك بالإفصاح عنها. كما يجب أن تشتمل هذه الخطة على ما هو أكثر من مجرد مخاطر متعلقة باستمرارية الأعمال، التي تحدثنا عنها بإيجاز في الفصل العاشر من هذا الكتاب، بل يجب أن تشتمل أيضاً على ضوابط خاصة لمنع القراصنة hackers من الوصول إلى ملفات البيانات، ومنع الموظفين الموتورين أو الناقمين من الوصول إلى معلومات العملاء، ومنع أي تهاون حتى لو كان بسيطاً. كما تطلب قاعدة الأساليب الوقائية الخاصة بقانون GLBA من كل مؤسسة مالية، بغض النظر عن حجمها، بل وتفرض عليها بأن تقوم بوضع وتنفيذ خطة مكتوبة لأمن المعلومات لحماية بيانات العملاء. بحيث يتناسب نطاق هذه الخطة الأمنية ودرجة تعقيدها تناسباً طردياً مع حجم المؤسسة وحساسية المعلومات التي تحتفظ بها. ويجب أن تكون هذه الخطة قائمة على عملية تحليل المخاطر التي تعمل على تحديد كل التهديدات المتوقعة بالنسبة لأمن وسرية وخصوصية وسلامة معلومات العملاء. وبناء على هذه العملية التحليلية للمخاطر، فإنه ينبغي على المؤسسات المالية توثيق وتطبيق التدابير والإجراءات الأمنية، التي تتضمن أيضاً التدابير والإجراءات الإدارية مثل تدريب الموظفين على وسائل الحماية التقنية، متضمناً ذلك تدريبات حول استخدام كلمات المرور وضوابط التشفير والجدران النارية. كما تشتمل هذه التدابير والإجراءات الأمنية كذلك على الاحتياطات الوقائية المادية مثل الأقفال الموجودة على الأبواب وأجهزة الحاسب الآلي. كما يجب على المؤسسات المالية أن تقوم بتخصيص واحد أو أكثر من موظفيها لكي يقوم بتنسيق وتنظيم تلك الأساليب الوقائية. كما يتعين على تلك المؤسسات أيضاً القيام بإجراء مراجعات دورية لتحديد ما إذا كانت البرامج الأمنية المتبعة فيها جيدة أم بحاجة إلى تعديل في ظل الظروف المستجدة.

تستطيع المؤسسة أن تثبت امتثالها للقاعدة الخاصة بالأساليب الوقائية من قانون GLBA من خلال الخطوات التالية:

١- **تحليل المخاطر البيئية المحيطة:** يجب على المؤسسة أن تحدد بشكل رسمي جميع المخاطر الداخلية والخارجية المتعلقة بأمن وخصوصية وسلامة المعلومات الشخصية

لجميع العملاء. وقد سبق الحديث عن الطرق التحليلية للمخاطر في الفصل الثامن من هذا الكتاب. ويجب أن تغطي تلك العملية التحليلية مخاطر أو فقدان أو الإفصاح عن جميع مصادر المعلومات الشخصية، سواء كانت موجودة على الأنظمة الآلية أم في السجلات اليدوية.

٢- **تصميم وتطبيق الإجراءات الوقائية:** إن الإجراءات الوقائية هي بالأصل عبارة عن إجراءات الرقابة الداخلية التي تم الحديث عنها في الفصل الرابع من هذا الكتاب كجزء من إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO).

٣. **المتابعة والتدقيق:** يجب أن تكون هناك عمليات متابعة مستمرة لضمان القيام بعمليات التدقيق. كما يتعين على الإدارة العليا تشجيع مدققيهم الداخليين بأن يضعوا جدولاً زمنياً منتظماً لسلسلة من المراجعات للتحقق من مدى ملاءمة أو كفاية خطة أمن المعلومات في المؤسسة إلى جانب اختبارات الامتثال المناسبة.

٤. **برنامج ثابت للتحسينات:** نتيجة منطقية لأي نقطة ضعف أو ثغرة يتم الإبلاغ عنها من خلال عمليات التدقيق أو أي فحوصات أخرى، فإنه يجب أن يكون لدى المؤسسة برنامج معمول به يعمل بشكل مستمر على إجراء التحسينات اللازمة على خطة أمن المعلومات لديها. ويجب أن يكون هذا البرنامج موثقاً جيداً وأن يصف التحسينات التي طرأت على الخطة.

٥. **الإشراف على مزودي خدمات أمن المعلومات والشركاء:** قد يكون للعديد من الشركاء والمؤسسات الأخرى أحقية الوصول إلى المعلومات الشخصية تلك نفسها، أو ربما يكون لديهم فقط إمكانية الدخول إلى وصلات شبكات النظم التي يمكن من خلالها انتهاك الخصوصية الشخصية للبيانات. فهناك حاجة لسياسات وضوابط وإجراءات تدقيق ملاءمة معمول بها على نحو جيد لمنع الانتهاكات.

تُطَبق قاعدة الأساليب الوقائية لقانون GLBA على مجموعة كبيرة من مزودي المنتجات والخدمات المالية، متضمنين وسطاء الرهن العقاري وجهات الإقراض غير المصرفية والمثمنين ووكالات إعداد التقارير الائتمانية ومعدي الضرائب المهنية، هذا بالإضافة إلى تجار التجزئة الذين يقومون بإصدار بطاقات ائتمانية خاصة بهم وبأعمالهم. ولا تَخْضَع البنوك لقاعدة

الأســاليب الوقائية الخاصة بقانون GLBA، ولكنها يجب أن تمتثل للوائح تنظيمية مناظرة أو مشابهة لها قد تم إصدارها من قِبل الوكالات الاتحادية للأعمال المصرفية. وقد ينتج عن عدم الامتثال لقاعدة الأســاليب الوقائية لقانون GLBA فرض الغرامات أو بعض الإجراءات التنفيذية من قبل هيئة التجارة الفيدرالية (Federal Trade Commission (FTC.

قوانين حظر التحجج الاحتيالي pretexting في قانون GLBA:

يمنــع قانون GLBA "التحجج الاحتيالي" - ذلك التعبير الذي يشــير إليه المدقق الإملائي في برنامــج معالــج النصوص وورد Word على أنه خطأ إملائي - والذي يقصد به اســتخدام الادعاءات والأســاليب الكاذبة، متضمناً ذلك اســتخدام البيانات المزورة، أو القيام بانتحال شخصية ما من أجل الحصول على المعلومات المالية الشخصية الخاصة بالعملاء، مثل معرفة الأرصــدة البنكية الخاصة بهم. حيــث يقوم المزورون أو المخادعون باســتخدام مجموعة متنوعة من الأســاليب للحصول على المعلومات الشــخصية. على ســبيل المثــال، قد تقوم إحدى المخادعات بإجراء مكالمة هاتفية تدعي فيها العمل لدى شركة تقوم بإجراء دراسات اســتقصائية، ثم تقوم بطرح بعض الأســئلة التي تهدف من خلالها إلى الحصول على اســم أحــد البنوك على ســبيل المثال، ثم تقوم بعد ذلك باســتخدام تلــك المعلومات التي قامت بالحصــول عليها لتقوم بإجراء مكالمة هاتفية مع المؤسســة الماليــة التي تحتفظ بمعلومات الشخص المستهدف متظاهرة بأنها هي ذلك الشخص المستهدف أو بأنها هي الشخص الذي يملك صلاحية الوصول إلى حسابه. وقد تدعي بأنها نسيت دفتر الشيكات الخاص بها وأنها بحاجة لمعلومات عن الحساب. فبهذه الطريقة قد تتمكن تلك المخادعة من الحصول على بعض المعلومات الشــخصية للضحية المســتهدفة كرقم الضمان الاجتماعي أو رقم الحساب البنكي أو رقم بطاقة الائتمان أو معلومات عن التقارير الائتمانية أو وجود وحجم المدخرات الشخصية والمحافظ الاستثمارية.

وبموجب أحكام قانون GLBA الخاصة بالادعاءات الاحتيالية، فإنه من غير القانوني لأي شخص:

- أن يســتخدم بيانــات أو وثائق مزورة أو وهمية أو مخادعــة للحصول على أي معلومات شخصية للعملاء من المؤسسة المالية أو من عميل المؤسسة المالية بشكل مباشر.

- أن يستخدم وثائق مزيفة أو مفقودة أو مسروقة للحصول على معلومات العميل من المؤسسة المالية أو بشكل مباشر من عميل المؤسسة المالية.
- أن يطلب من شخص آخر الحصول على معلومات عميل ما باستخدام بيانات كاذبة أو وهمية أو احتيالية أو باستخدام وثائق مزورة ووهمية ومخادعة أو وثائق مسروقة أو مفقودة أو مزيفة.

تؤدي مثل تلك الادعاءات الاحتيالية إلى نوع جديد من المخاطر المتعلقة بالأمن والخصوصية، أو يمكن القول بأنها ستعرضنا إلى ما يعرف بسرقة الهوية Identity Theft. ويحدث هذا عندما يقوم شخص ما بسرقة المعلومات التعريفية الشخصية الخاصة بك لفتح حسابات سداد جديدة أو لطلب سلع ومنتجات أو للقيام باقتراض الأموال. وعادة لا يكتشف هؤلاء الضحايا المستهدفون من قِبل لصوص الهويات الشخصية بأنهم ضحايا حتى يعجز هؤلاء السارقون عن دفع فواتير أو سداد قروض وتبدأ جهات التحصيل بمطالبة الضحايا المستهدفين بتسديد الحسابات التي لا علم لهم بها أصلاً. ووفقاً لهيئة التجارة الفيدرالية FTC فإن النماذج الأكثر شيوعاً في سرقة الهويات هي:

- **الاحتيال على بطاقات الائتمان:** فتح حساب بطاقة ائتمان باسم مستهلك ما أو الاستيلاء على حساب بطاقة ائتمان موجود بالفعل.
- **الاحتيال في خدمات الاتصالات:** يقوم سارق الهوية بطلب خدمة هاتف أو هاتف نقال أو غيرها باسم المستهلك.
- **الاحتيالات البنكية:** فتح حساب سواء كان جارياً أم ادخارياً باسم مستهلك ما وكتابة شيكات مزورة.
- **القروض الاحتيالية:** يقوم سارق الهوية بطلب قرض ما كقرض شراء سيارة مثلاً باسم مستهلك آخر.

هناك قانون اتحادي مستقل مرتبط بقانون GLBA ألا وهو قانون منع سرقة الهوية والادعاءات الواهية The Identity Theft and Assumption Deterrence Act ، والذي اعتبر بأنه يعد جريمة فيدرالية أن يقوم شخص ما بشكل متعمد وبدون أي سلطة قانونية

بنقل أو باستخدام الوسائل التعريفية الخاصة بشخص آخر بقصد ارتكاب نشاط غير قانوني أو التحريض عليه، وأن ذلك يشكل انتهاكاً للقانون الفيدرالي، ويعتبر أيضاً جناية وفقاً لأي قانون يمكن تطبيقه على مستوى الولاية أو محلياً. يعد كلٌ من الاسم أو رقم الضمان الاجتماعي "وسائل تعريفية"، وكذلك الأمر بالنسبة لرقم البطاقة الائتمانية أو الرقم التسلسلي الإلكتروني للهاتف الخلوي أو أي جزء آخر لمعلومات قد تستخدم بمفردها أو بالاشتراك مع غيرها من المعلومات لتحديد هوية شخص محدد.

قانون GLBA هو أحد القوانين التي بمقدورها التأثير على العديد من كبار المديرين، خاصة هؤلاء الذين يعملون في المؤسسات المالية على اختلاف أنواعها. وحيث إن العديد من جوانب قانون GLBA تهدف بالمقام الأول إلى حماية المعلومات المالية للعملاء، فقد أصبح الأمر الدارج إلى حد كبير هو أنه من المحتمل أن يكون لقانون GLBA آثار على مجموعة كبيرة من المؤسسات في الولايات المتحدة. لذا يجب على المؤسسات المالية والمانحة للائتمان أن تكون أكثر إدراكاً لقواعد قانون GLBA وقواعد الخصوصية العامة التابعة له والتي يمكن تطبيقها على العديد من المؤسسات الأخرى. وتعتبر شبكة الويب هي المصدر الأفضل بشكل مطلق للحصول على معلومات إضافية تفصيلية وحديثة عن قانون GLBA وأحكامه. وهناك مصدران جيدان لهذا الغرض هما:

١- **لجنة التجارة الاتحادية:** يقدم هذا المصدر الحكومي نظرة عامة على قانون GLBA ومعظم قواعده الحالية. على الرابط التالي:

http://business.ftc.gov/privacy-andsecurity/gramm-leach-bliley-act

٢- **الجمعية الوطنية لمفوضي التأمين:** وهي مؤسسة تنظيمية توجد في كل ولاية على حدة، حيث تمتلك كل مؤسسة من هذه المؤسسات التنظيمية معلومات عامة عن قانون GLBA يمكن الاطلاع عليها عن طريق زيارة الموقع www.naic.org، هذا بالإضافة إلى العديد من مواقع الويب الأخرى التي تغطي مواضيع ذات صلة بشكل تفصيلي.

على الرغم من أن قانون GLBA لا يزال أحد العناصر الهامة في تشريعات الولايات المتحدة، فإنه ظل إلى حد ما بعيداً عن الأنظار منذ عام ٢٠١١ في ظل المتطلبات المعقدة لما يعرف بقانون دود فرانك Dodd-Frank. حيث يعمل هذا القانون على تنفيذ التغيرات

التـــي، من جملة أمور أخرى، تؤثر في العمليات الرقابية والإشرافية على المؤسســات المالية، وتقدم أيضاً إجراءات حازمة جديدة للشركات المالية الكبرى، وإنشاء وكالة جديدة مسؤولة عن تنفيذ وفرض الامتثال للقوانين المالية التي تخص المســتهلك، وطرح متطلبات رأسمالية تنظيميــة أكثر قوة، والمســاهمة في إحــداث تغيرات كبيرة وهامة في اللائحــة التنظيمية لما يســمى بالمشتقات المالية، وتعديل اللوائح التنظيمية الخاصة بوكالات التصنيف أو التقييم الائتماني، وإحداث تغيرات على حوكمة الشركات والممارسات التنفيذية للتعويضات، واشتراط تسجيل المستشارين للحصول على تمويل خاص، والمساهمة أيضاً في إحداث تغيرات كبيرة في ســوق التورق. أي أنه بمعنى آخر، يمكن القول إن هذا القانون قد أحدث الكثير من الأمور والتغيرات.

يعتــبر هذا القانــون واحداً من العناصر المعقدة في التشريع وقد تمت صياغة المســودة الخاصــة ببنــود هذا القانــون في الوقت الذي كان فيه هذا الكتــاب تحت الطباعة. ومن خلال استطلاعنا المحدود على هذا التشريع، تبين أن لهذا القانون بعض الاهتمامات المباشرة في حوكمــة تقنية المعلومــات. في جميع الأحوال يعد هذا القانــون عنصراً آخر من عناصر التشريع التي أسهمت في وضع قواعد جديدة للعديد من المؤسسات هذه الأيام.

قانون إخضاع التأمين الصحي لقابلية النقل والمحاسبة (HIPAA): العناية الصحية وأكثر:

ســيُطلب من المديــر المقيم في الولايات المتحدة الذي يقوم بزيــارة الطبيب هذه الأيام لإجــراء الفحوصات الســنوية أو لأي إجراءات أخرى أن يوقع على ما يشــبه موافقة خطية تهدف إلى الســماح بالإفصاح عن معلوماته، وذلك قبل الشروع في عمل الفحوصات، وذلك أثناء قيامة بإجراءات حجز الكشف عند وصوله مكتب الاستقبال. حيث يتم بموجب هذه الوثائق الحصول على موافقة المريض أو المريضة على الســماح بمشــاركة الســجلات الطبية الخاصة به أو بها أو الإفصاح عنها على أنها جزء من الإجراءات الخاصة بهذه الزيارة الطبية. وإذا قام هذا المدير المريض بالســؤال عن ســبب ذلك الإجراء، تكون الإجابة غالباً بأن هذا الإجراء هو "أحد المتطلبات القانونية الخاصة بقانون HIPAA". ويكون رد الفعل الطبيعي للمريــض عادة هو القيام بالتوقيع على تلك الوثائق المطلوبة والاســتمرار بالإجراءات دون أن يكــون هناك فهم تام للغايــة الحقيقية من الحصول على هذا التوقيع. فعلى الرغم من

مجموعــة القواعد الخاصة بالعناية الصحية الواردة في قانــون HIPAA، فإنه يحتوي أيضاً على قواعد تشريعية أخرى تتعلق بالخصوصية، تذهب إلى ما هو أبعد من العناية الصحية، وسوف تؤثر في العديد من المؤسسات وكذلك المدققين الداخليين التابعين لها.

يتطلب العمل في الولايات المتحدة الأمريكية سواء كان ذلك في شركة صناعية أو مؤسسة خدمــات ماليــة أو الكثير غيرها ، أن يكــون لدى كبار المديرين مســتوى فهم وإدراك عام لقانون HIPAA وقواعده. فقد صدر هذا القانون عام ١٩٩٩م، وتم إصدار القواعد النهائية له خلال الســنوات اللاحقة لتلك الســنة. وقد كان لقانــون HIPAA أثر كبير في الولايات المتحدة الأمريكية في خصوصية وأمن معلومات الســجلات الطبية الشــخصية وعلى العديد من السجلات الشخصية الأخرى. يتعرض الأفراد لقانون HIPAA عند قيامهم بزيارة إحدى العيادات الطبية الخاصة بأحد الأطباء أو عند تعرضهم للعديد من المســائل الطبية الأخرى المتعلقة بالأمور الطبية. كما تشــهد أيضاً إدارات الموارد البشرية في المؤسســات أثر ونتائج متطلبــات قانــون HIPAA هذه الأيام على إدارتها لســجلات مخططــات الرعاية الصحية والمعالجات الطبية الخاصة بالموظفين لديها. ومن المؤكد أن هذا القانون قد تسبب أيضاً في إحداث آثار كبيرة ومتزايدة وبدرجة غير مســبوقة على مجمل قطاع الرعاية الصحية وعلى جميــع مقدمــي خدمات الرعاية الصحية التابعين له. والأهــم من هذا كله أن قواعد هذا القانون قد شملت مجموعة كبيرة من عمليات الأعمال القائمة على التجارة الإلكترونية.

لهذا القانون التشريعي الأساسي أربعة أهداف:

١- التأكيد على إمكانية نقل التأمين الصحي من خلال إزالة القيود والشروط الوظيفية التي كانت موجودة في الســابق. وقد كان ذلك بمثابة المحفــز الرئيسي الذي أدى إلى إقرار قانون HIPAA. حيث كان في الســابق يتم إجراء العمليات التشخيصية والفحوصات اللازمة للأشــخاص في ظروف وتحت شروط معينــة، ولكن بعد ذلك كان أغلب هؤلاء الأشــخاص لا يســتطيعون الحصول على تغطيات صحية جديدة عنــد قيامهم بتغيير الجهات التي يعملون بها، وذلك لأن عملية مشاركة المعلومات المتعلقة بتلك الحالات الصحية الخاصة بهؤلاء الأشــخاص مع الآخرين كانت في كثير من الأحيان تتم بشــكل غير مرن.

٢- الحـد من عمليات الغـش والاحتيال وسـوء المعاملة في كل ما يتعلـق بأمور الرعاية الصحية. فقد أدت تلك الكلمات التي تم طرحها في جلسـات الاستماع الخاصة داخل الكونجرس الأمريكي عندما تم الاستشـهاد ببعض الأمثلة عن الاحتيال وسـوء المعاملة المزعومة إلى تشريع هذا القانون.

٣- فـرض معايـير خاصة بالمعلومـات الصحية. وقد تـم تغطية ذلك مـن خلال قواعد الخصوصية والأمن الواردة في قانون HIPAA والتي سنوجزها لاحقاً.

٤- ضمان أمن وخصوصية المعلومات الصحية.

سـيقدم هذا القسـم نظرة عامة وموجزة عن أهداف قانون HIPAA والقواعد الناتجة عنه، والتي تغطي مسـائل حوكمة وخصوصية وأمن تقنية المعلومات. وعلى الرغم من عدم طرح جميع الجوانب والقضايا المتعلقة بقانون HIPAA في هذ الكتاب، فإننا نتحدث عنه هنا عـلى أنه قانون تشريعي آخر تقوده "القواعد الجديدة" التي لا تزال تؤثر في العديد من كبار المديرين في المؤسسات. إن التقدم الذي حدث في هذا القانون التشريعي يوضح ويفسر آليات العمل المتبعة لوضع وإقرار القوانين التي تتم تحت رعاية وإشراف الجهات الحكومية المعنية. في البداية، كان الإصدار الأول لقواعد قانون HIPAA على شـكل مسودة تابعة لأحد اللوائح التـي كانـت قد نشرت في وقت مبكـر. وقد كان هناك العديد مـن الملاحظات والتعليقات الموجـودة على تلك المسـودات، وكان لا يزال هناك المزيد من الملاحظـات والتعليقات على مسـودات لقواعد منقحة ومحسـنة تم إصدارها لاحقاً، وقد تم إصدار نسخ القواعد الأخيرة الخاصة بهذا القانون في وقت متأخر جداً عما كان مخطط له في الأصل.

قواعد الخصوصية لسجلات المرضى وفقاً لقانون HIPAA:

كانت الاهتمامات والمخاوف المسـتمرة المتعلقة بمسـائل الخصوصيـة الطبية للمرضى من الأسـباب التحفيزية الرئيسـية التي جعلت الكونجرس الأمريكي يوافق على إقرار قانون HIPAA. فعندمـا نقوم بزيارة إحدى المراكـز المتخصصة بتقديم خدمات الرعاية الطبية، لمناقشـة بعض المخاوف أو مشكلة ما، فإننا نتوقع بعد ذلك أن تتم المعالجة بطريقة سرية وخاصة للغاية. فنحن لا نرغب مثلاً في أن يتم إرسـال النتائج الخاصة بالزيارات التي قمنا

بهـا للمراكز والعيادات الطبيـة إلى إدارة الموارد البشرية التابعة للأماكـن التي نعمل بها، أو أن يتم إرسـال تلك النتائـج لإحدى شركات التأمين التي لا تربطهـا أي علاقة بالموضوع وليسـت بحاجة لمعرفة تلك النتائج، أو أن يتم ترك تلك النتائج على أحد مكاتب الاستقبال الخاصة بمقدمي الخدمات الطبية ليقوم بعد ذلك شـخص ما بالتقاطها والتصرف فيها بكل سهولة. والأسوأ من هذا كله، هو أننا لا نرغب في أن تتم مشاركة تلك النتائج أو المعلومات أو أي مسـائل شـخصية وسرية بصورة قد تحد من فرص وخيارات التوظيف المسـتقبلية الخاصـة بنا. هذا الخوف أو القلق المرتبط بمسـألة خصوصية المعلومات الشـخصية، هو السـبب الأسـاسي وراء العديد من قواعد قانون HIPAA. من ناحية أخرى، فهناك العديد مـن الأطراف التي ترغب في الحصول على معلومـات تتعلق بشروط الرعاية الصحية لدينا لتقديم تغطية صحية وتعويضات مالية ملائمة، ومن الناحية العملية فإنه يمكننا القول بأن جميع العمليات التشغيلية الخاصة بتقديم خدمات الرعاية الصحية تحتاج إلى نظم داعمة تفصيلية ومعقدة جداً. وتغطي قواعد قانون HIPAA خمسـة مجالات عامة سـنتحدث عنها جميعاً بشـكل موجز في الفقرات التالية. إن هذه الفقرات هنا لا تقدم تغطية شاملة لقواعـد هذا القانون، وليس الغرض منها هـو أن تكون مصدراً مرجعياً لتلك القواعد، وإنما تهـدف إلى إعطاء المهنيين من خارج القطاع الطبي لمحة عامة عن القواعد الجديدة التالية الخاصة بقانون HIPAA.

١- **اسـتخدامات السـجلات الطبية والإفصاح عنها:** ينبغي على المؤسسة الخاضعة لقواعد قانون HIPAA أن تتخذ الخطوات اللازمة للحد من استخدام المعلومات الطبية الشخصية والإفصـاح عنها ليكون ضمن "الحد الأدنى الـذي لا بد منه لإنجاز وإتمام الغاية التي من أجلهـا تم اسـتخدام تلـك البيانات أو الإفصاح عنهـا أو طلبها" في القضايـا والأمور غير العلاجية. وسـنبدأ في طرح النظرة العامة عن قواعد قانون HIPAA بكلمات وعبارات مقتبسـة بشـكل مباشر من نصوص تلك القواعد، كاسـتخدام عبارة "the minimum necessary" بمعنى "الحد الأدنى اللازم" في الجملة السـابقة. حيث يحتوي القانون على العديد من الأمثلة الخاصة بهذه الإرشادات التوجيهية المتعلقة بالممارسات التي تختارها المؤسسـة لـكي تتحقق من مدى صحتها من خلال الاطلاع عـلى أحكام وتداعيات أخرى سابقة كانت قد وقعت على مر السنين.

جاء هذا القســم من قواعد قانون HIPAA لتوضيح أن المعلومات الصحية الشــخصية الخاصة بشــخص ما ســتفقد حماية هذا القانون HIPAA لها في حال كان هناك نقص في المُعرِفات الخاصة بهذا الشــخص المعني بهذا القانون، كعدم احتواء تلك المعلومات الصحية عــلى أي من المحــددات أو المعرفات الثمانية عشر الخاصة بمعلومات حول هذا الشــخص وعلاقاتــه أو علاقاتها وأصحاب العمل وأفراد أسرته أو أسرتها. إن هذا المطلب يقول الكثير عن قانون HIPAA. فلتحقيق الامتثال لنظام المعلومات الصحية الخاص بقانون HIPAA، قام هذا القانون التشريعي بتحديد تلك الثمانية عشر معاملاً التي يجب أن يســتخدمها أي أخصــائي تقنية معلومات أثناء قيامه بتنفيذ عمليات اســترجاع البيانات من قاعدة البيانات بهــدف تحديد هوية شــخص ما. هذا يعني، أنه ســواء كانت المعلومــات الطبية الخاصة بشــخص ما موجــودة في ملف أو في نظام معلومــاتي محمي ضد عمليــات الإفصاح العام للآخرين، فإنه من الممكن مشاركة تلك المعلومات مع الآخرين في ظروف وشروط معينة.

٢- **متطلبات التفويض أو التصريح:** هذا القســم في HIPAA هو الذي يتعرض له معظم مســتخدمي خدمــات الرعاية الصحية. لــذا يجب أن يحصل مقدمــو خدمات الرعاية الصحية على موافقة خطية تتعلق بالسماح لهم بالإفصاح عن جميع المعلومات الخاصة بالرعاية الصحية باســتثناء بعض حالات الطوارئ. وللشخص الحق في عدم الموافقة على مثــل هذا الأمر الذي يتعلق بالإفصاح أو الكشــف عن معلوماتــه الطبية، وهناك شرط حاســم وقوى يفرض على مقدمي خدمات الرعاية الصحية القيام بالاحتفاظ بالسجلات الضروريــة للقيام بتتبع جميع العمليات المتعلقة بهذه الإفصاحات. وكما ذكرنا ســابقاً، فــإن هــذا هو ما يُطلب من الشــخص التوقيع عليــه عند قيامه بزيارة أحــد المراكز أو العيادات الطبية من خلال تقديم مجموعة من الوثائق التي تحتاج إلى توقيعه.

٣- **نشر الممارســات المتعلقــة بالخصوصية:** يجب أن يكون لــدى مقدمي خدمات الرعاية الصحية ممارسات وإجراءات منشورة للخصوصية التي ينبغي عليهم توفيرها لمستخدمي المستفيدين من خدمات الرعاية الصحية المقدمة. بعد ذلك يحق للأفراد أن يطلبوا بشكل رسمي المزيد من القيود والمحددات التي يرغبون فيها على تلك السياسات المتبعة، ويجب على مقدمي الخدمات الصحية استيعاب جميع الطلبات المعقولة والمنطقية للمستخدمين.

٤- **حقوق الوصول للســجلات الطبية والتعديل عليها:** للأشــخاص الحق في فحص أو نسخ (جزئي أو كلي) للمعلومات الصحية الشخصية الخاصة بهم. كما أن لديهم الحق في طلب إجراء تعديلات مناســبة على تلك الســجلات الصحية الخاصة بهم. كما يجب أن يقوم مقدمو الرعاية الصحية بالاحتفاظ بسجلات عن جميع الأطراف التي طلبت الوصول إلى تلك السجلات الشخصية للمعلومات الصحية الخاصة بهم خلال الشهور الستة الأخيرة.

٥- **إدار الخصوصية في قانون HIPAA:** بالذهاب إلى ما هو أبعد من قواعد الوصول للسجلات والإفصاح عنها، فإن لدى قانون HIPAA مجموعة واســعة من المتطلبات المتعلقة بإدارة الخصوصيــة. ويتم تطبيق هذه المتطلبات أو القواعد على ما يعرف بالكيانات المشــمولة "Covered Entities" كالعيادات الطبية والمختبرات والمستشفيات وكل ما له علاقة بأمور الرعاية الصحية الشخصية. وتشتمل القواعد الخاصة بإدارة الخصوصية على ما يلي:

- ينبغي على مقدم خدمات الرعاية الصحية تعيين "موظف خصوصية "Privacy Official يكون مسؤلاً عن الأمور المتعلقة بالخصوصية، بحيث يكون هو المعني بقضايا تطوير وتطبيق تلك الإجراءات والسياسات الخاصة بقانون HIPAA.
- ينبغي على مقدم خدمات الرعاية الصحية أن يقوم بتدريب أعضاء كادر العمل أو الموظفين لديه على التعاطي مع سياسات وإجراءات قانون HIPAA المتعلقة بالخصوصية، كما يجب عليه الاحتفاظ بالوثائق التي تثبت بأن هذه التدريبات قد تمت فعلاً.
- ينبغــي على مقدم خدمات الرعاية الصحية أن يمتلك ضمانــات وتدابير أمنية، وإدارية، وفنية، ومادية معمولاً بها لحماية خصوصية المعلومات الصحية الشخصية.
- ينبغــي على مقدم خدمــات الرعاية الصحيــة تطبيق "العقوبات المناســبة Appropriate sanctions" على الموظفين غير الملتزمين بتلك الإجراءات والسياسات المتعلقة بالخصوصية.
- ينبغــي عــلى مقدم خدمــات الرعاية الصحية إيجــاد وتطبيق السياســات والإجراءات المصممــة لتحقيق الامتثال أو الامتثال لعناصر موجودة في اللوائح التنظيمية الخاصة بقانون HIPAA. كما يجب الاحتفاظ بتلك الوثائق الرســمية لمدة ستة أعوام، سواء كانت مكتوبة على أوراق أم على شكل نماذج إلكترونية.

وعلى الرغم من أن تلك القواعد الخاصة بقانون HIPAA تشــمل بالمقام الأول عمليات الوصول للمعلومات الصحية الشخصية، فإنها ذكرت مجالات أخرى تحدد ممارسات تشغيل جيــدة يجــب أن يتم تطبيقها في أي مــكان آخر في داخل المؤسســة. والمثال على ذلك هو تضمينها لــشرط الاحتفاظ بالوثائق المتعلقــة بالبرامج التدريبية التي تــم إنجازها من قبل مقدمي خدمات الرعاية الصحية. فقد تم وضع هذا النوع من القواعد أو المطالب في البداية للبرامــج الطبية للإدارة الاتحادية للعقاقــير أو برامج الدواء. أما الآن فإن هذه القواعد تمثل جزءاً أساســياً من قانون HIPAA وتعتبر فكرة جيدة بالنســبة لمعظــم البرامج التدريبية في الشركات. فالمؤسسات في بعض الأحيان تنفق الكثير من مواردها الخاصة في تدريب موظفيها إلا أنها لا تكلف نفسها غالباً عناء القيام بتوثيق هذا النشاط التدريبي على نحو جيد.

إن لهــذه القواعد وغيرها مــن القواعد المذكورة في هذا الفصل أهمية خاصة بالنســبة للمســؤول التنفيــذي الذي يعمل في إحدى المؤسســات التي لها علاقة بالمســائل المتعلقة بالرعاية الصحية كالمستشفيات أو شركات التأمين الطبي. فضلاً عن أن هذه القواعد تتسع وتمتــد لتصــل إلى مجالات أخرى مثل معالجــة المطالبات الخاصة بالتأمــين الطبي في إدارة الموارد البشرية لإحدى المؤسسات، أو المتعلقة بسلامة مرافق المصنع والتبليغ عن الحوادث الصناعية. يجب أن يكون لدى جميع المؤسسات المعنية بقضايا الرعاية الصحية أيضاً قواعد وإجــراءات امتثال قوية لقانــون HIPAA، إلا أن تقديم وصف تفصيلي لمثل هذه القواعد والإجراءات المتبعة ليس من ضمن نطاق وأهداف هذا الكتاب. على كل حال فإن الامتثال لقانون HIPAA يعد أيضاً مطلباً في العديد من البيئات الأخرى. يوضح الشكل التوضيحي (١١-٣) بعض إجراءات حوكمة تقنية المعلومات فيما يخص قانون HIPAA التي يجب أن تكون موجودة ومفعلة في أي مؤسسة خاضعة لقانون HIPAA.

التشفير ومتطلبات الأمن في قانون HIPAA:

بالإضافة إلى قواعد الخصوصية المتعلقة بالتفويض والإفصاح عن الســجلات الطبية، فإن قانــون HIPAA يحتوي أيضاً على بعض متطلبات أمن تقنية المعلومات التي تم تحديدها بدقــة والتــي يصعب تطبيقها في العديد من المؤسســات الصغيرة. فهــو يدفع على حدود الممارســات الأمنية لتقنيــة المعلومات (زيادة حجم الممارســات الأمنية التقنية) بالنســبة

للعديد ويحتاج بعض الأمور كالقيام بتأمين التوقيعات الإلكترونية على الرغم من محدودية التقنيات الناضجة أو الفعالة فنياً المســتخدمة حالياً لتوفير مثل هذه التوقيعات الإلكترونية الآمنة في ظل وجود الشــبكات المفتوحة كشبكة الإنترنت. فنحن لا زلنا في المرحلة التي قد يتمكن فيها أحد القراصنة المهرة لنظم الحاســبات من اعــتراض أو اختراق إحدى مكالمات الهاتف الخلوي التي تتناول بعض المواضيع والمســائل المتعلقة بالمعلومات الخاصة بالرعاية الصحية، الأمر الذي يعتبر بمثابة اختراق لمتطلبات الأمن والسرية لقانون HIPAA. ستتغير التقنية في المســتقبل وستتحســن إجراءات الضبط والرقابة وســيزداد ذكاء وخبرة القراصنة وسيتم تسوية هذه الاختراقات والانتهاكات في المحاكم.

لقد كان الســبب الرئيسي وراء وضع مثل تلــك القواعد السرية هو عدم ملاءمة وكفاية العديــد من نظم إدارة تقنية المعلومات الخاصة بالرعاية الصحية التي كانت موجودة قبل قانون HIPAA. ففي كثير من الأحيان نرى أن المؤسسات يمكنها تحسين هذه النظم الأمنية لا عن طريق شراء وتركيب برمجيات جديدة فحسب، بل عن طريق تحسين السياسات التي يقودهــا البشر أولاً. وقــد تم الانتهاء من قواعد المعايير الأمنيــة الخاصة بقانون HIPAA ووضعهــا حيز التنفيذ في شــهر إبريل من عام ٢٠٠٣. إلا أنــه لم يتم تفعيل معايير الامتثال لتلــك القواعد حتــى عام ٢٠٠٦. ومن بين المجالات الأخرى التي تشــملها هذه القواعد ما يطْلِق عليه قانون HIPAA اسم "الوحدات المشمولة Covered Entities" والتي تشمل:

- الأطبــاء وغيرهم من الذين يقومــون بتقديم خدمات الرعاية الصحيــة والذين يقومون بمعالجة مطالبات الرعاية الصحية بشكل إلكتروني.
- الخطط الصحية بما فيها مؤسسات التأمين الذاتي.
- دور المقاصــة الخاصة بالخدمــات الصحية - لخدمات الفواتــير وغيرها والذين يقدمون خدمات تهيئة البيانات الخاصة بالمطالبات الإلكترونية المقدمة.

شكل توضيحي (١١-٣)

المتطلبات والإجراءات الخاصة بحوكمة تقنية المعلومات في قانون HIPAA.

١. يجب أن يتم تعريف المؤسسة على أنها أحد المؤسسات المعنية بتقديم خدمات الرعاية الصحية والخاضعة لقانون HIPAA. (إن كان هذا غير متوفر، فليس هناك حاجة لاستكمال باقي الخطوات).
٢. للامتثال لقانون HIPAA وللخطة التنفيذية العامة الموضوعة لهذا القانون، فلا بد من تعيين موظف رسمي مسؤول عن أمن المعلومات المتوفرة على مستوى المؤسسة.
٣. لا بد من وضع وتنفيذ سياسات وإجراءات لحماية المعلومات الصحية الخاصة بالمرضى.
٤. يجب أن يكون هناك عمليات معمول بها للقيام بعمليات الدعم والرقابة المستمرين لقواعد قانون HIPAA ولوائحه.
٥. يجب أن تتضمن عمليات قانون HIPAA سياسات وإجراءات وضوابط وتقنيات شاملة فيما يتعلق بمسائل الخصوصية والأمن.
٦. لا بد أن يكون للمؤسسة خطة رسمية للطوارئ معمول بها تتضمن ما يلي: • التحليلات الحساسة للتطبيقات والبيانات. • خطط النسخ الاحتياطي للبيانات. • خطط التعافي من الكوارث Disaster Recovery. • خطة للعمليات التشغيلية خلال حالة الطوارئ. • الفحص والتنقيحات الدورية المقترحة للخطة.
٧. يجب أن تشتمل عمليات قانون HIPAA على عمليات رسمية لضبط الوصول إلى البيانات، والتي تتضمن أيضاً العمليات المتبعة للحصول على إذن الوصول للبيانات وقواعد إنشاء الاتصال بالبيانات والإجراءات اللازمة لتعديل الوصول إلى البيانات.
٨. يجب أن تشتمل الضوابط الموضوعة لمراقبة عمليات الوصول إلى الوسائط الخاصة بنظم المعلومات على العمليات التالية: • المساءلة. • نسخ احتياطية للبيانات. • تخزين البيانات. • التخلص من البيانات.

٩. يجب على الإجراءات أو السياسات الأمنية الشخصية أن: • تضمن الإشراف على موظفي الصيانة من قبل شخص مطلع ومفوض بذلك. • تحتفظ بسجلات كاملة عن التصريح بالوصول للمعلومات. • تضمن حصول موظفي التشغيل والصيانة على تفويض أو إذن وصول مناسب. • توفير إجراءات إجازة الموظفين .
١٠. يجب أن يكون هناك إجراءات رسمية معمول بها لإنهاء الخدمات، والتي تتضمن تغيير مجموعة مناسبة من الأقفال والإزالة من قوائم الوصول أو الحصول على البيانات.
١١. يجب أن تشتمل ضوابط الوصول الفعلي للنظم والمعلومات في جميع أنحاء المؤسسة على: • خطط عمليات التشغيل في حالة الطوارئ. • مراقبة وضبط المعدات داخل وخارج المنشأة. • خطط أمن المرافق. • إجراءات التحقق من تصاريح الوصول قبل الوصول الفعلي إلى النظم والبيانات. • سجلات الصيانة. • الإجراءات اللازمة لمعرفة عمليات الوصول للنظم والبيانات بالنسبة للذين يصرح لهم ذلك. • تسجيل الدخول للزوار والمرافقين إذا كان ذلك مناسباً. • فحص وتنقيح خطة الوصول الفعلي للبيانات.
١٢. يجب حماية جميع الشبكات والاتصالات من خلال: • الخروج التلقائي. • الهوية الفريدة للمستخدم. • كلمات المرور وأرقام التعريف الشخصية PINs. • أنظمة الرد الهاتفية.

يعنـــي ذلــك أن قواعد الأمن والسريـــة الموجودة في قانـــون HIPAA يتم تطبيقها على جميع المؤسسات، سواء كانت عبارة عن عيادة يوجد بها طبيب واحد أم مستشفى كبيراً أو مكتبــاً صغيراً متخصصاً في معالجة المطالبات الخاصة بقضايا الرعاية الصحية التابعة لها من خلال التأمين الذاتي.

قواعــد الأمن والسرية هي العنــصر الرئيسي في قانـــون HIPAA المعني بالحفاظ على خصوصيـــة المعلومات الصحية الشــخصية. وتغطـــي هذه القواعد ممارســـات جيدة فيما يتعلــق بالأمن والسريـــة لما هو أكثر بكثير من مجرد حماية للســجلات الطبية، كالمتطلبات الخاصــة بالمعايير القوية للتعافي من الكوارث. تحتوي القواعد المنشـــورة لقانون HIPAA عــلى نوعين من القواعد هما: قواعد مطلوبة أو إلزاميـــة "Required" وقواعد غير إلزامية "Addressable" كــما أطلق عليها القانون. هذا النـــوع الأخير يمثل القواعد التي لا يُطْلَب من المؤسســـة القيام بتنفيذها أو تطبيقها نظراً لصغر حجمها أو قلة مواردها. أما القواعد الإلزاميـــة لقانون HIPAA فتمثل العديد من الممارســـات الجيدة في مجال أمن المعلومات التي تناســـب جميع المؤسســـات. هناك مجالات أمن أخرى في قانون HIPAA لكنها خارج نطـــاق وأهداف هذا الكتـــاب، كالمتطلبات الخاصة في بيئة البنية التحتية الرئيســـية العامة والتي تتضمن التوقيعات الرقمية.

الإجراءات الإدارية الأمنية لتقنية المعلومات في قانون HIPAA:

يحتـــاج قانـــون HIPAA إلى إجـــراءات إداريـــة معمول بهـــا لحماية ســـلامة البيانات وخصوصيتها وإتاحتها. ويجب أن يتم توثيق هذه الإجراءات بحرص وعناية لكل قاعدة من قواعـــد قانون HIPAA. يعرض الشـــكل التوضيحي (١١-٤) بعض هذه الإجراءات الإدارية الإلزامية "Required". كما يوضح هذا الشـــكل أيضاً القواعد التنفيذية لكن بطريقة عامة جداً، أما بالنســـبة للقواعد المنشـــورة لقانون HIPAA فقد جاءت بشكل أكثر تفصيلاً. إن العديد من هذه المتطلبات كخطة الطوارئ الموثقة والمختبرة أو السياسات الرسمية لضوابط الوصـــول للمعلومات، تكون مشـــابهة لإجراءات الضبط والرقابة التـــي أوصى بها المدققون الداخليون على مر السنين. بعضها يمثل الممارسات الجيدة في حوكمة تقنية المعلومات التي ينبغي أن تكون معمولاً بها في العديد من المؤسسات. على سبيل المثال، يشير الشرط رقم ٣

في الشـكل التوضيحي (١١-٤) إلى الحاجة إلى ما يسمى سياسة العقوبات – وهي مجموعة رسـمية من القواعد التي تُطبق على الأشـخاص الذين يخترقون سياسـة الأمن. إنها لفكرة جيدة بالنسبة إلى معظم المؤسسات هذه الأيام، وكقاعدة إدارية، أن يتعرض مقدم خدمات الرعايـة الصحية الخاضع لقانون HIPAA للجزاءات إذا تم اكتشـاف عدم ملاءمة وكفاءة القواعد والإجراءات المتبعة لديه.

وتشتمل المتطلبات الأمنية لقانون HIPAA أيضاً على القواعد الوقائية المادية المشابهة لضوابط الوصول الفعلي للبيانات التي كانت موجودة على مراكز البيانات الخاصة بتقنية المعلومات والتي تعود إلى الأيام الأولى لأجهزة الحاسبات المركزية الضخمة mainframe. في جميع الأحوال، استطاع قانون HIPAA هنا أن يتخطى حدود مركز عمليات التشغيل التقليـدي لتقنية المعلومات، ويدعو إلى إيجاد إرشـادات توجيهيـة ووثائق قوية تتعلق باسـتخدام محطة العمـل والموقع. وعلى الرغم من أنه قد جـرت العادة ألا تقوم إدارة تقنية المعلومـات ومدققوها الداخليون بإثارة العديد من المخاوف لدى الرقابة الداخلية التي تتعلق بالضوابط المادية للأجهزة الطرفية المتصلة من خلال الربط الشـبكي في البيئة الخاصة بمنشـأة الأعمال، إلا أن بيئات العنايـة الصحية الخاضعة لتنظيم قانون HIPAA تطرح العديد من القضايا الجديدة. فقد تكون محطة عمل البيئة الطبية التي ربما يكون فيهـا أطباء وممرضون وغيرهـم من الموظفين، بحاجة إلى ضوابـط منطقية ومادية قوية لحماية الخصوصية الشـخصية لسجلات المرضى التي يمكن أن يتم تسريبها من خلال تلك المحطات.

شكل توضيحي (١١-٤)

المواصفات المطلوبة لتطبيق قانون HIPAA

أحكام للوحدات المشمولة "Covered" كجزء من خطة الأمن والامتثال لقانون HIPAA.
١. تحليـل المخاطر: يجب على المؤسسـات إجراء تقييم أو تقدير كامـل للمخاطر المحتملة المتعلقة بسرية وسلامة وإتاحة البيانات.
٢. إدارة المخاطـر: يجب على المؤسسـات المشـمولة تطبيق تدابير أمنية ملائمـة ومعقولة للحد من المخاطر وإبقائها ضمن المستوى المقبول (لتكون تحت السيطرة).
٣. سياسـة العقوبـات: لا بـد من تطبيق العقوبات والجـزاءات على أعضاء الـكادر الوظيفي الذين يخترقون السياسـات الأمنية المتعلقة بالخصوصية في المؤسسة، كتطبيق سياسة من نوع "ثلاثة أخطاء، إذاً أنت مطرود من العمل" (وهي السياسـة التي تفرض المزيد من العقوبات على هؤلاء الأشـخاص الذين يدانون بجريمة خطيرة علماً أنهم كانوا قد أدينوا سابقاً باثنتين من القضايا الخطيرة أيضاً).
٤. الإبلاغ عن إعداد تقارير بشأن نشاط أمن نظم المعلومات: لا بد من التبليغ عن سجلات أمن المعلومات وتقارير الحوادث وغيرها من التقارير المتعلقة بالأنشطة الأمنية والقيام بمراجعتها بشكل منتظم.
٥. إجـراءات الاسـتجابة للحوادث: لا بد مـن وجود عمليات معمول بها لتحديـد الحوادث الأمنية والتحقيق فيها والتخفيف من آثارها وتوثيقها.
٦. إجراءات النسخ الاحتياطي: لا بد من وجود إجراءات معمول بها للتعافي من أي خسارة أو فقدان للبيانات.
٧. التعافي من الكوارث: ينبغي على كل مؤسسة مشمولة بالقانون أن تقوم بوضع الإجراءات المناسبة التي تغطي أي فقد للبيانات.
٨. حالة الطوارئ الخاصة بعمليات التشغيل: لا بد من وجود عمليات معمول بها لضمان أمن وسرية معلومات المرضى عندما يكون التشغيل في حالة الطوارئ.
٩. العقود التجارية ذات العلاقة. يجب على المؤسسـة تضمين أسلوب في عقود الموردين يشترط على المورد تبني تدابير أمنية كافية للإبلاغ عن الحوادث الأمنية التي تقع في المؤسسة وضمان تطبيق المقاولين الفرعيين (مقاولي الباطن) للتدابير الأمنية الملائمة وفسخ العقد في حال تبين وجود أي اختراقات أمنية.
١٠. التخلص من معلومات المريض: لا بد من وجود سياسات وإجراءات معمول بها لمعالجة الأرشفة النهائية لمعلومات المريض وحفظها.

١١. إعادة استخدام الوسائط: لا بد من توفير العمليات المعمول بها لضمان إزالة المعلومات الحساسة من الوسائط الإلكترونية كمشغلات الأقراص قبل القيام بإعادة استخدامها.
١٢. معرف فريد لهوية المستخدم: يجب تخصيص محددات أو معرفات فريدة لجميع مستخدمي النظم لمنع مشاركة الحسابات ولتتبع سلوك النظام.
١٣. إجراءات الوصول للبيانات في حالة الطوارئ: لا بد من إيجاد إجراءات تسمح بالوصول إلى المعلومات الإلكترونية في حالات الطوارئ.
١٤. التوثيق: لا بد من إيجاد إجراءات لضمان أمن وسرية المعلومات والحفاظ على الوثائق لمدة ست سنوات ومراجعتها بشكل دوري.

الخدمات والآليات الخاصة بالأمن التقني:

تتطلب قواعد قانون HIPAA وجود عمليات معمول بها لحماية سلامة وسرية وإتاحة بيانات السجلات الطبية ومنع الوصول غير المصرح به لأي من البيانات المرسلة عبر شبكات الاتصال المستخدمة. تحتاج هذه القواعد غالباً إلى ضوابط أكثر قوة وصرامة من تلك الموجودة في بعض المؤسسات الكبيرة. وتتضمن هذه الضوابط الأمور التالية:

- **ضوابط الوصول إلى البيانات:** لا بد من إيجاد آليات رقابية قوية تعتمد على سياق البيانات أو دور أو مركز المستخدمين المصرح لهم. هذا بالإضافة إلى العمليات الرقابية التي يجب دائماً أن تكون في موضع التنفيذ للسماح بالحصول على البيانات في حالات الطوارئ بواسطة العمليات التشغيلية لمركز البيانات إذا تطلب الأمر.
- **ضوابط التدقيق:** يوجد مطالبات هنا وفي جميع القواعد الأخرى لقانون HIPAA بضرورة وجود ضوابط تدقيق قوية، والتي تتضمن وجود أمور كعمليات التنقيح أو التعديل للتوثيق وعمليات مراقبة الآثار والمسارات التقليدية الخاصة بالتدقيق.
- **اعتماد صحة البيانات:** هناك حاجة إلى ضوابط نظم قوية لحماية وسلامة البيانات.
- **اعتماد الكيان:** لا بد من وجود ضوابط معمول بها بحيث أنه عندما تحاول إحدى محطات العمل الوصول إلى محطة عمل أخرى، فلا بد أن يكون مصرحاً لها القيام بذلك.

وقد تتضمن هذه العملية اســتخدام ضوابط لكلمات المرور أو الرد الآلي على الهاتف أو حتــى ضوابط المقاييس الحيوية. لقد تخطى هذا المطلب حدود الكثير من ممارســات المؤسسات المطبقة هذه الأيام، حيث يتم مشاركة أو تبادل البيانات بكل سهولة وحرية من خلال رسالة البريد الإلكتروني ومرفقاتها.

• **ضوابط الاتصالات والشــبكة:** هناك مجموعة واســعة مــن الضوابط المقترحة هنا مثل التنبيهات والتشــفير والإبلاغ عن الأحداث والتصديق على الرســائل وغيرها. يجب على المؤسسة الخاضعة لقانون HIPAA أن تقوم بتنفيذ شبكة آمنة جداً.

يقتضي قانون HIPAA أن تمنح الضوابــط الخاصة بالتوقيع الإلكتروني البيانات الموقعة إلكترونياً الوزن القانوني نفســه للمســتندات الورقية التي وقع عليها توقيعاً تقليدياً. حيث ينص قانون HIPAA على سلامة الرسائل الشبكية وعدم إنكار واعتماد المستخدم لأي رسالة تحتوي على توقيع إلكتروني. وقد يشــكل هذا تحدياً إضافياً بالنسبة للعديد من الأشخاص. وتســتخدم اليوم عمليــات التوقيع الرقمي أو الإلكتروني، إلا أنهــا مرهقة بعض الشيء ولن تكون إلزامية حتى يتم تطوير تقنيات جديدة أفضل لضمانها.

أســهمت قواعد قانون HIPAA في تقدم العديد من المجالات المتعلقة بأمن وســلامة تقنية المعلومات. وعلى الرغم من أن هذه القواعد قد وُجِدَت من أجل المؤسسات المعنية بتقديم خدمات الرعاية الصحية، فإنها ستؤثر في العديد من المؤسسات الأخرى. لذا يتعين على كبار المسؤولين التنفيذيين محاولة الحفاظ على مستوى عام من المعرفة الخاصة بتلك القواعــد الســارية ومعاييرها المطلوبة حتى وإن كانوا لا يعملون بشــكل مباشر في إحدى مؤسسات تقديم خدمات الرعاية الصحية. وقد قمنا في هذا الفصل بتقديم نبذة مختصرة جــداً عــن تلك القواعد المعقدة والهامة في الوقت نفســه. وبالذهاب إلى ما هو أبعد من مجرد مؤسســات الرعاية الصحية، فإن هذه القواعد تطبق أيضاً كلما كان هناك ســجلات مرتبطــة بالأمــور الصحية يتم الاحتفاظ بها من قبل إدارة الموارد البشرية. ويســتطيع أي مديــر مهتم أن يحصل على المزيد مــن المعلومات المتعلقة بقانــون HIPAA من هذين المصدرين الهامين:

١. **U.S. Department of Health and Human Services (وزارة الصحـة والخدمات البشرية الامريكية):** نسخ من قواعد قانون HIPAA ووسائل دعم مرجعية أخرى يمكن الحصول عليها عن طريق زيارة الموقع:

www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

٢. **HIPAA Advisories (الإرشـادات الخاصـة بقانـون HIPAA):** وهو موقع تشرف عليـه نظم فونيكس Phoenix الصحية كموقع خدمات عام، ويعتبر واحداً من المصادر الجيـدة للحصـول على معلومات عن قانـون HIPAA والموجود في العنـوان: http:// www.phoenixhealth.com

يعـد الامتثال لقواعـد قانون HIPAA مطلبـاً قانونياً في الولايات المتحـدة الأمريكية. ولأن مدققـي الحكومة لا يقومون بزيارة المستشـفيات أو مرافـق الرعاية الصحية الكبيرة ومن المؤكد أيضاً أنهم لا يقومون حتى بزيارة إدارات الموارد البشرية الخاصة بالمؤسسـات التجارية، فالشخص الذي يشعر أن هناك انتهاكاً أو اختراقاً لهذا القانون، يستطيع أن يتقدم بشكوى مباشرة إلى وزارة العدل الأمريكية (Department of Justice (DOJ. وقد يحدث هذا بالتأكيد عندما تصبح بعض المعلومات الرئيسية الموجودة في سجلات الموظف الخاصة بالتعويضات المطلوبة من شركات التأمين مكشـوفة ومعروفة للعموم بسبب اختراقات أمن وسرية تلك السجلات. فلدى وزارة العدل الأمريكية DOJ نهج الامتثال الطوعي للشكاوى.

لـذا ينبغـي على كبار المديريـن المهتمين أن يكونـوا على دراية ومعرفـة ولو على أقل تقدير بالمستوى الرفيع أو الخطوط العريضة لقواعد قانون HIPAA وبقضايا حوكمة تقنية المعلومات المرتبطة بها. فهم أحد الأسـباب القوية الأخرى لجعل المؤسسـة تقوم بتطبيق ضوابط قوية تتعلق بـالأمن والخصوصية في أي مجال من شأنه أن يؤثر في السجلات الطبية أو الصحية الخاصة بالموظفين.

ملاحظات:

1. Privacy Rights Clearinghouse (PRC), https://www.google.com/#hl=en&sclient=psyab&q=privacy+rights+clearinghouse&oq=Privacy+Rights+Clearinghouse+&gs_l=serp.1.3.0l3j0i30.0.0.1.9354.0.0.0.0.

2. "The State of PCI Compliance," Forrester Consulting, September 2007, www.rsa.com/solutions/PCI/ar/RSA_AR_State_of_PCI_Compliance.pdf.

3. العديد من المحتويات الخاصة بمشاكل TJX's يمكن العثور عليها، مثل

"T.J. Maxx Data Theft Worse Than First Reported," MSNBC.com, March 29, 2007, www.msnbc.msn.com/id/17853440/ns/technology_and_science-security/t/tj-maxx-data-theft-worse-firstreported/#.Tp2

4. Robert Moeller, IT Audit, Control, and Security (Hoboken, NJ: John Wiley & Sons, 2010).

الفصل الثاني عشر
بيان خدمات تقنية المعلومات: تحقيق قيمة أكبر من عمليات تشغيل تقنية المعلومات

كما تحدثنا في الفصول السابقة، كان المستخدمون في الأيام الأولى لنظم تقنية المعلومات يلجؤون إلى مديري قسم تقنية المعلومات أو الموظفين المسؤولين عن النظم لديهم ومطالبتهم بأن يقوموا بإجراء تعديلات أو ترقيات للنظم القائمة حالياً أو أن يقوموا بإطلاق نظم جديدة. وقد كانت معظم تلك المطالب لا تتعدى كونها تقارير ورقية جديدة أو تقارير بصيغ وأشكال مختلفة. وقد اشتكى هؤلاء المستخدمون في كثير من الأحيان من سوء خدمات تقنية المعلومات إما بسبب تأخير تسليم مشاريع النظم التي قاموا بطلبها أو لأن تلك النظم المنجزة لم تكن على مستوى توقعاتهم أو لوجود العديد من المشاكل الأخرى. وكان ذلك قبل ظهور الإنترنت، أي في الأيام التي كانت فيها نظم وخدمات تقنية المعلومات محدودة جداً. وقد جرت العادة بأن يقوم هؤلاء المستخدمون بتلخيص جميع احتياجاتهم واستكمال نموذج من نماذج الطلبات الرسمية الخاصة بخدمات تقنية المعلومات التي يرغبون فيها. ثم يقوم قسم تقنية المعلومات بمراجعة الطلبات المقدمة والتي كانت في الغالب يتم التصديق عليها ووضع جدول زمني لإتمامها في أقرب وقت ممكن - أحياناً يكون الوقت المحدد للبدء في تنفيذ الطلب مناسباً وقريباً من وقت تقديم الطلب، ولكن في كثير من الأحيان يكون غير مناسب ومتأخراً كثيراً عن وقت تقديم الطلبات.

أما اليوم فإن خدمات تقنية المعلومات تعد أكثر تعقيداً من كونها مجرد تقارير مالية وتشغيلية والتي كان يتم تقديمها بصورة منتظمة في السنوات الماضية. في كثير من الأحيان نرى أن مستخدمي النظم هذه الأيام بحاجة إلى إجراء تحاليل من نوع خاص تعتمد على مخرجات أنظمة أخرى قائمة بالفعل. وقد يكون لدى مستخدمي النظم بعض الاحتياجات المتعلقة بتوقيت إجرائي استثنائي تفرضه متطلبات رفع تقارير قانونية دولية، أو قد يكون لديهم اهتمام بإحدى التقنيات الجديدة التي شاهدوها في إحدى العروض التجارية

ويرغبون في مشـاهدة مثلها في المؤسسة التابعين لها. ويكون هناك غالباً العديد من النظم والأدوات المتاحة لدى إدارات تقنية المعلومات، إلا أن أعضاء إدارات مجتمع المستخدمين لا يكونـون غالباً على علم بخدمات تقنية المعلومات المتاحة من خلال إدارة تقنية المعلومات في المؤسسـة التابعين لها. وعلى غرار قائمة الطعام التي تقدم إلينا عند زيارة أحد المطاعم، فإن قسم تقنية المعلومات يستطيع أن يساعد مجتمع المستخدمين لديه عن طريق تقديم قائمة أو بيان بالخدمات التقنية المتاحة لديهم. ويستفيد مستخدمو موارد تقنية المعلومات غالباً مـن قراءة البيانات الخاصـة بخدمات تقنية المعلومات عندمـا يقومون بطلب تلك الخدمات أو جدولتها.

إن بيان خدمات تقنية المعلومات IT service catalog عبارة عن قائمة بالخدمات التي ينبغي على قسـم تقنية المعلومات في المؤسسة أن يقدمها للموظفين والعملاء وغيرهم من أصحـاب المصالح. وتحتوي عادة كل خدمة من خدمات تقنية المعلومات التي يتم وصفها في بيان كهذا على ما يلي:

- **وصف الخدمة:** وهي قائمة بتطبيقات أو عمليات تقنية المعلومات الموجودة في الخدمة والتي قد يحتاج إليها المستخدم في إدارته. ويجب أن تتناسب هذه التطبيقات مع مجمل العمليات التشغيلية للأعمال ومتطلبات النظم الأخرى الخاصة بها.
- **الأطـر الزمنيـة أو اتفاقيات مسـتوى الخدمة (SLAs) اللازمة لاسـتيفاء الخدمة:** تعد اتفاقيات مسـتوى الخدمة من المعاملات الثنائية (تحتوي على طرفين) التي تأخذ شـكل اتفاق داخلي أو عقود غير رسـمية بين إدارة تقنية المعلومات والمستخدمين. وتعتبر هذه الاتفاقيات من الأدوات الهامة جداً في حوكمة تقنية المعلومات التي سـيتم الحديث عنها بمزيـد من التفصيل في الفصل السـابع عشر من هذا الكتـاب. الفكرة هي أنه يجب أن يُذكر في بيان خدمات تقنية المعلومات الوقت الذي سيتم فيه تسليم الخدمة المشار إليها ومتطلبات إدارة المستخدم للوفاء بعروض الخدمة هذه.
- **من الذي يحق له طلب أو عرض الخدمة:** يجب أن يحدد البيان مثلاً أن هناك مجموعات خاصة من التقارير التحليلية ستكون متاحة فقط لمستويات وظيفية محددة في الإدارات المالية. وبالمثل، قد تقوم بعض الخدمات المعروضة في البيان بالنص على أن المستخدمين

الذين يطلبون تلك الخدمات يجب أن يتحملوا بشكل رسمي مسؤولية حل بعض الأخطاء أو القيام ببعض المراجعات لمخرجات نظم محددة.

- **تكاليـف الخدمات التقنيـة:** إن فكرة أن يتم تقديم خدمـات تقنية المعلومات كموارد "مجانية" داخل المؤسســة قد انتهت منذ زمن بعيد. وسـيقوم الفصل الســابع عشر من هذا الكتاب بتقديم بعض الدعم الإضافي لحوكمة تقنية المعلومات لإدارة وفهم التكاليف والتسعير. ومع ذلك يجب أن يحدد بيان خدمات تقنية المعلومات بعض الإرشادات التي تتعلق بتكاليف الخدمات المعروضة في البيان.
- **كيفية الوفاء بالخدمة المذكورة في البيان:** ينبغي أن يكون هناك بعض المعلومات بشــأن توقيت تســليم الخدمة ومســتويات الموافقة المطلوبة وغيرها مــن المعلومات الضرورية المتعلقة بالخدمة المطلوبة من البيان.

على الرغم من أن بيان الخدمات يُعتبر واحداً من الأدوات الهامة بالنسبة لإدارات تقنية المعلومــات، فإنــه أيضاً مهم وذو قيمة بالنســبة للعديد مــن الإدارات الأخرى غير العاملة في تقنية المعلومات وحتى بالنســبة للعروض المتعلقة بإدارة الموارد البشرية. فعلى ســبيل المثال، يمكن اســتخدام تطبيق عرض خدمة لتسجيل استحقاقات الموارد البشرية للموظف أو تغييرها أو تعديل الاشــتراكات أو المصروفات من حســابات الإقراض أو حسابات الادخار للموظف، أو الإقرار بالموافقة على مدونة قواعد السلوك الخاصة بالموظف.

يمكن لإدارات تقنية المعلومات في المؤسســة أن تقوم بنشر عروض الخدمة لديها بشكل فعال من خلال موقع المؤسســة على شبكة الإنترنت والمتاح فقط لأصحاب المصلحة المصرح لهم. يســتطيع المســتخدم بعد ذلك القيام بزيارة الموقع للبحــث عن خدمة محددة مثل طلب جهاز حاســب آلي محمول جديــد، أو طلب تعديل الاســتحقاقات، أو القيام بإضافة موظف جديد في أحد الأقسام في المؤسسة. يقوم هذا الموقع الخاص ببيان الخدمات بإعادة تجميع الخدمات المعروضة حسب الفئات أو الأصناف التي تنتمي لها ويسمح باستخدامها في عمليــات البحــث (خاصة عندما يكون هناك مئات بــل آلاف الخدمات المتاحة). حيث يقوم المســتخدم باختيار الخدمة التي يريدها ومشــاهدة الوصف والتفاصيل المتعلقة بها. كما يقوم المســتخدم بإدخال أي معلومات تتعلق بالخدمات، كمعلومات الاتصال أو أسئلة

متعلقــة بالخدمة، ثم يقــوم بتقديم طلب للحصول على الخدمــة المطلوبة. يحتاج طلب الخدمــة إلى الموافقــة أو التصديق عليه، ثم يمــر من خلال عملية التوجيــه وعملية إدارة مستوى الخدمة وغيرها من العمليات اللازمة لاستيفاء الطلب. يستطيع المستخدم العودة إلى الموقــع لاحقاً لفحص حالة الطلب أو لاســتعراض جميــع المقاييس المتعلقة بمدى نجاح الإدارة في أداء الخدمات التي تقدمها.

يعــد بيان خدمــات تقنية المعلومات أحــد الأدوات القيّمة والهامة للحوكمة بالنســبة للعديــد من المؤسســات. يأخذ هذا الفصل بعين الاعتبار كيفيــة وضع وتطبيق بيان فعال لخدمات تقنيــة المعلومات، كما يأخذ بعين الاعتبار أيضاً بعض الضوابط الرئيســية اللازمة لتحســين عمليات حوكمة تقنية المعلومات ذات العلاقة. ونظراً لأن إدارة تقنية المعلومات هي التي تقوم بوضع المعايير والضوابط لتحديد الموارد التي يجب إدراجها على أنها خدمات لتقنيــة المعلومات في بيان خدمــات تقنية المعلومات الخاص بهــا، ولأن هذا البيان يعمل على تحديد الخيارات المتاحة للمجتمع المســتخدِم لتقنية المعلومات المؤسســية، فإن بيان الخدمات المنظم والمحكم جيداً يمكن اعتباره أحد العناصر الهامة في الحوكمة الفعالة لتقنية المعلومات.

أهمية بيان خدمات تقنية المعلومات:

نظــراً لزيــادة الطلب من قبل وحدات الأعــمال لخدمات جديــدة في تقنية معلومات ولمســتويات أعلى للخدمة، وكذلك الضغوط المســتمرة للتكاليف، فقــد قامت العديد من وحــدات التشــغيل الكبيرة لتقنية المعلومات المؤسســية بإجراء تحــولات وتغيرات جذرية خاصة في الســنوات الأخيرة. فقــد أدرك الرئيس التنفيذي للمعلومــات (CIO) وغيره من المســؤولين التنفيذين لتقنية المعلومات أن هناك حاجة إلى تحقيق مواءمة أو توافق أفضل بين الخدمات التي يقدمونها واحتياجات العمل، وإلى تحســين رضا العميل الداخلي، ونشر عمليات معيارية لتحقيق كفاءة تشــغيلية أكبر. إن هذا الإصرار على تحســين جودة الخدمات - وإظهــار قيمة الأعمال - قد دفع العديد من إدارات تقنيــة المعلومات إلى تطبيق عمليات محســنة للخدمات، مثل عمليات آيتل والتي تمت مناقشــتها في الفصل الســادس من هذا الكتاب، بالإضافة إلى بعض المنهجيات الأخرى لعملية تقنية المعلومات. ويعد بيان خدمات

تقنية المعلومات أحد المكونات الرئيسـية والذي تدعو الحاجة إليه لتحسـين خدمة عملاء تقنية المعلومات.

ويعتمـد إطار العمل آيتل عـلى المفاهيم الخاصة بالعناية بخدمـات تقنية المعلومات وعملائهـا. حيث يكون بيان خدمـات تقنية المعلومات في قلب تلك المفاهيم الأساسـية. وقد انتجت العديد من إدارات تقنية المعلومات بيان الخدمة كجزء من نشر إدارة مستوى الخدمـة طبقـاً للإطار آيتل. على أية حال، حتى لو كانت المؤسسـة إلى الآن لم تتبن جميع مفاهيـم آيتل، فقد يكون بيان الخدمات المؤسسـية بمثابة نقطة محورية لتحقيق التفاعل بين تقنية المعلومات والأعمال، كما يمكن أن يمنح كل منهما فرصة تحسين الخدمات المقدمة لعملاء تقنية المعلومات. إن بيان خدمة تقنية المعلومات يعد أحد الأدوات الهامة لحوكمة تقنية المعلومات، كما أنه ضروري أيضاً لتوفير الأسـاس من أجل تحديد الخدمات والتواصل مع الأعمال.

ولـكي يكون بيـان خدمات تقنيـة المعلومات فعـالاً، فإنه يجب أن يُفهـم ويتم تبنيه واسـتخدامه من قِبل الأعمال. لقد أصبحت بيانات خدمات تقنية المعلومات هي المفهوم الجديد "الساخن" منذ بضع سنوات، إلا أننا نجد غالباً أن إدارات تقنية المعلومات تستهلك سـاعات طويلة لتقوم بإنشـاء وثيقة بيان الخدمات الخاصة بها، مسـتخدمةً في ذلك صيغاً ثابتة وجامدة ولا يقوم بقراءتها أو استخدامها إلا عدد قليل من العملاء. لذا نجد أن العديد من بيانات الخدمة الثابتة هذه من النادر أن يراها أو يقرؤها المستخدمون أو صناع القرار - وتصبح غالباً في نهاية المطاف عديمة التأثير.

ولـكي يتم بناء بيـان فعال لخدمات تقنيـة المعلومات، فإنه يتعين عـلى مديري تقنية المعلومـات بالإضافة إلى مديري وحدات الأعمال في المؤسسـة أن يقوموا بتحديد الخدمات التي سـيتم إطلاقها لمستخدميهم النهائيين من خلال بيان الخدمة الخاصة بهم. وقد جرت العادة أن يقوم مديرو وحدات الأعمال ومحللو تقنية المعلومات بتحديد أنواع الأسئلة التي يمكن أن تُطرح من قبل مسـتخدمي بيان الخدمات الخاص بهم، وأن يقوموا أيضاً بتحديد الموافقـات اللازمة لطلـب الخدمات، وأن يذكروا أيضاً النظـم والعمليات الأخرى المطلوبة لاسـتيفاء الطلب. فبمجـرد أن يتم تحديد الخدمة وتنظيم عملية اسـتيفائها، فإنه ينبغي

عـلى إدارة تقنية المعلومات بناء جميع الوظائف الضرورية داخل تعريف الخدمة ومن ثم نشرها في بيان الخدمة.

إن مصطلح خدمة العملاء ليس جديداً بالنسبة للعمليات التشغيلية لتقنية المعلومات. فضلاً عن أنه في الأيام الأولى لنظم التقنية وعملياتها التشغيلية، كان قسم تقنية المعلومات في أغلب الأحيان هو الذي يقرر ما الذي يجب "تطبيقه" ومتى سيتم تطبيقه. إن التكاليف الباهظة للخدمات والنظم السـيئة وعدم رضا المستخدمين عنها والتي لا تلبي احتياجاتهم، قد أدت إلى إعادة التفكير بشكل كبير من جانب إدارة تقنية المعلومات فيما يخص الخدمات التي تقدمها لمستخدميها. وقد أسهم نمو نظم الحاسبات الشخصية والإنترنت في تغيير تلك المفاهيـم عبر السـنين. أما اليوم فإن العديد مـن إدارات تقنية المعلومـات وكذلك إدارة المؤسسـة بدؤوا يدركوا أنهم في الأساس ما هم إلا وحدة لخدمة العملاء، فهم يعملون على تقديـم الدعم اللازم للنظم وغيرها مـن موارد تقنية المعلومات لجميع إدارات المؤسسـة التابعين لها. لقد أصبح بيان الخدمة أحد السـمات الرئيسـية للمساعدة في بناء الخدمات الخاصة بعملاء تقنية المعلومات ودعمها. على كل حال، ولكي نضمن وجود مبادرة ناجحة لخدمات تقنية المعلومات تركز على العملاء، فإنه يجب على إدارات تقنية المعلومات اتباع التوجيهات الثلاثة التالية لبناء وتطوير بيان لخدمات تقنية المعلومات:

١- **الإقرار بأن مسـتخدم التقنية هو الملك:** بداية وقبل كل شيء يجب أن يتم إنشـاء بيان بخدمـات تقنية المعلومات مع التركيز القوي على حاجات العملاء الداخليين. إن الخطأ الأكـثر شـيوعاً الذي تقع فيه معظـم إدارات تقنية المعلومات هـو محاولة التركيز أكثر عـلى شرح الخدمات التي يقدمونها من منظور تقنيـة المعلومات. فعادة لا يكون لدى عملاء تقنية المعلومات الرغبة في استعراض أوصاف تفصيلية للخدمة من خلال "عبارات تقنية". بل يرغبون بمشـاهدة شروحات للخدمات المقدمة بعبارات يسـتطيعون فهمها ومكتوبة بمصطلحات غير تقنية، ومعالجة الشواغل أو الاحتياجات العاجلة.

يتـم تحديد البيانـات الناجحة لخدمات تقنية المعلومات اعتـماداً على العميل وتأثيره داخل المؤسسـة بدلاً من البنيـة التحتية من حيث تأثيرها في الخارج. وكناحية إرشـادية، فـإن البيانات الناجحـة لخدمات تقنية المعلومات يجب بناؤها بطريقة مشـابهة للبيانات

الحقيقية الموجودة عبر الإنترنت والتي تستخدم يومياً من قبل العملاء. مثل بيانات الخدمة الخاصة بأمازون دوت كوم Amazon.com، ودل Dell ، وإي باي eBay.

يجب أن يشبه بيان خدمات تقنية المعلومات أحد هذه البيانات الخاصة بالعملاء والمنشورة على شبكة الإنترنت. وذلك من خلال استخدام توصيفات سهلة الفهم وواجهة استخدام سلسة لاستعراض جميع عروض الخدمات المتاحة في البيان. يعمل البيان الفعال لخدمات تقنية المعلومات أيضاً على تقسيم العملاء الذين يحق لهم الوصول إلى البيان— سواء كانوا مستخدمين أم مسئولين تنفيذيين لوحدات الأعمال— ويقوم بعرض محتوى مختلف بناء على الإدارة، والأدوار، والاحتياجات، والمواقع، والصلاحيات. إن هذا النهج المعتمد على العميل في وضع البيان يساعد على ضمان تبني بيان خدمات تقنية المعلومات من قبل المستخدمين النهائيين وتوفير الأساس لنقاش متوازن لمستوى الأعمال فيما يتعلق بجودة الخدمة ومواءمات التكلفة مع صناع القرار في المؤسسة.

٢- **جعل بيان خدمات تقنية المعلومات قابل للتنفيذ:** من المهم ألا يكون بيان خدمات تقنية المعلومات أكثر من مجرد مستودع ثابت للمعلومات. فباستخدام المثال الذي طرحناه عن بيانات خدمات العملاء المنشورة على شبكة الإنترنت، حيث يقوم العملاء باستعراض البيان المنشور عبر الإنترنت على موقع أمازون. كوم Amazon.com أو دل. كوم Dell.com، وعند مشاهدتهم لشيء ما يريدونه، فبإمكانهم طلبه. بالمثل، يجب أن يرتبط بيان خدمات تقنية المعلومات المقدمة للمستخدمين النهائيين مع عمليات طلب الخدمة - وذلك من خلال واجهة عربة التسوق القائمة على الإنترنت والتي تُمَكِن المستخدمين النهائيين من طلب الخدمات وتتبع حالة الطلب عبر الإنترنت. على نحو مماثل، يجب أن يكون لدى مسئولي وحدات الأعمال التنفيذيين عرض فريد لبيان خدمات تقنية المعلومات الخاصة بالمؤسسة التابعين لها، وذلك لمنحهم مستوى أكبر من الشفافية على بنود ميزانية تقنية الأعمال ودوافع الاستهلاك ومستويات الخدمة وتأثير الأعمال على كل خدمة من الخدمات التي توفرها تقنية المعلومات.

تعد خدمات تقنية المعلومات أمراً هاماً بالنسبة للموظفين، وذلك عندما يرغبون في تحديث نظم الحاسبات المحمولة الخاصة بهم أو زيادة حجم صندوق البريد الإلكتروني

الخاص بهم. كما أنها تعد مسألة هامة بالنسبة لمسئولي الأعمال التنفيذيين عندما يقومون بمراجعة الميزانيات أو عند اســتلام فواتير تقنية المعلومات الخاصة بهم. هذه هي الأوقات التي يجب أن يكون فيها بيان خدمات تقنية المعلومات متاحاً وقابلاً للتنفيذ.

ولضــمان نجاح هذا الأمر، يجب أن يصبح بيــان الخدمات نقطة الوصول الوحيدة التي ســيلجأ إليها المســتهلكون في جميع احتياجاتهم المتعلقة بتقديم خدمات تقنية المعلومات الخاصة بهم، كما يجب أن يكون هذا البيان متاحاً وبســهولة تامة وفي أي وقت يحتاج فيه العملاء إلى التعرف على الأمور التي تنفذها تقنية المعلومات وكيف تقوم التقنية بتنفيذها. كل ذلك يعني أنه يجب على قسم تقنية المعلومات أن ينظر لخدمات تقنية المعلومات كما لو كانت سلعاً أو منتجات. إن كبار المديرين الذين كانوا على علاقة بإدارة تقنية المعلومات في الماضي كانوا يقومون وبشــكل رســمي بملء نوع مــن أنواع الوثائــق الخاصة بـ "طلب خدمــات تقنية المعلومات" وذلك عنــد الحاجة إلى تقرير جديد أو أحد العمليات الجديدة لتقنيــة المعلومات. وكانت هذه الطلبات في ذلك الوقت يتم تحويلها إلى نوع ما من أنواع اللجــان الإدارية التي كانت تقوم في البداية بمراجعة الطلبات المقدمة والموافقة عليها ومن ثــم تحديد أولويات التنفيذ. إن العديد من عمليات تقنيــة المعلومات اليوم لا تحتاج إلى نظــم مخصصة وأعمال برمجية كالتي كانت موجــودة في الماضي، بل يمكن تلبية احتياجات المستخدمين من خلال العديد من نظم وعمليات تقنية المعلومات الموجودة اليوم.

٣- **تمكين بيان خدمات تقنية المعلومات ليصبح نظام سجلات:** ينبغي أن يقوم بيان خدمات تقنية المعلومات القابل للتنفيذ بوظيفة "نظام للسجلات" الذي يجعل من الممكن إدارة وحدة خدمات تقنية المعلومات كما يدار مشروعٌ داخل مؤسســة. فبإمكان هذا البيان الخاص بخدمات تقنية المعلومات أن يوفر الوســائل والآليــات الضرورية لإدارة طلبات العمــلاء، وأن يناظر العمليات الخاصــة بتحقيق الخدمة مقابل كل خدمة من الخدمات المقدمة، وأن يضمن الامتثال لمستوى الخدمة والدفع بالكفاءات الخاصة بالعملية وتتبع التكاليف.

لا يمكــن لأي عمــل من الأعمال الموجهة نحو الخدمة أن يتم بشــكل فعال بدون توفير هذه البيانات المالية والتشغيلية بسهولة ويسر. فمن خلال تزويد العملاء الداخليين بنقطة

مركزية لطلب الخدمات، تستطيع تقنية المعلومات الاستفادة من هذه البيانات للتحكم في الاستهلاك بدرجة أكثر فاعلية. فمن خلال الخدمات القياسية والموثقة على نحو جيد، يمكن لفــرق تقنية المعلومات أن تفرض عمليات قابلــة للتكرار وقابلة للقياس لتقديم الخدمات، الأمــر الذي يــؤدي في نهاية المطاف إلى جودة يمكن التنبؤ بها وموثوقة بالنســبة لمســتوى الخدمات المقدمة. وهذا يســمح لمســئولي تقنية المعلومــات التنفيذيين من الحصول على المعلومات الضرورية لاســتخدامها في المناقشات المتعلقة بالأعمال والقائمة على الحقائق مع نظرائهم فيما يخص الميزانيات والتسعير.

يمكــن أن يكون بيــان خدمات تقنية المعلومــات حجر الزاوية للنجــاح في العديد من مبــادرات تقنيــة المعلومــات التي تركز على العمــلاء. فمن خلال تحديــد ونشر المحفظة المعياريــة الموحــدة الخاصة بعــروض الخدمات الخاصــة بالأعمال، تســتطيع إدارة تقنية المعلومات تســويق القيمة الخاصة بهــا بصورة أكثر فاعلية وتأســيس إطار عمل للتواصل مع الأعمال الأخرى. ومن خلال جعل بيان الخدمات تشــغيلياً وإجرائياً، تســتطيع عمليات تشــغيل تقنية المعلومات أن تساعد في توحيد عمليات استيفاء الخدمة، وإدارة الاستهلاك، ودفع عملية التحسين المستمر.

يمكن أيضاً وقف الخدمات التي لا يتكرر الطلب عليها باستمرار. وكذلك ينبغي تحسين العمليــات الخاصــة بتقديــم الخدمات كبيرة الحجــم، كما يمكن أن توفر مــؤشرات الأداء الرئيســية رؤية أكبر لضبط التكاليف، وضمان الجــودة الأفضل للخدمات المقدمة، وتقديم الدعم للنقاشات الخاصة بوضع الميزانية مع صانعي القرار.

من خلال بيان خدمات معمول به يركز على العميل وقابل للتنفيذ، يمكن لقســم تقنية المعلومــات أن يعمل بصفة مزود موجه نحو الخدمات حيث يقوم بتلبية احتياجات عملاء الأعمال لديه بشكل فعال. من ناحية أخرى، لا بد أن ندرك أن بيان خدمات تقنية المعلومات لا يجب أن يعرض أنواع الأشــياء الموجودة في بيان ســيرز ريباك Sears Roebuck catalog ذي الطراز القديم الذي كان موجوداً في الماضي — والذي كان يحوي العديد والمدهش من المدخــلات. لذا يجب أن يركز بيان خدمات تقنية المعلومــات على العروض الهامة لتقنية المعلومات في المؤسسة.

دور بيان الخدمة في تنظيم أعمال مزود خدمات تقنية المعلومات:

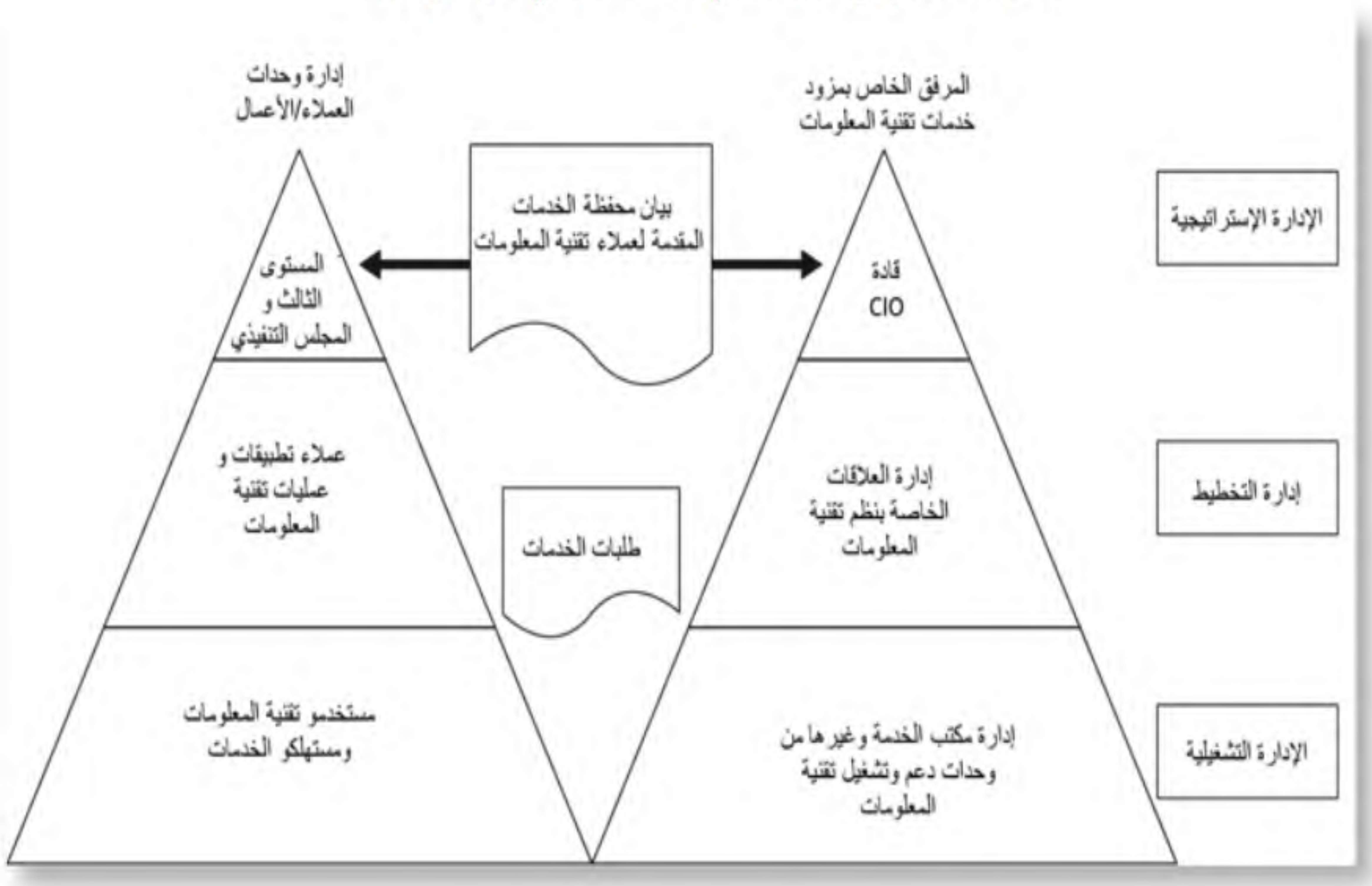
يجب أن يقدم بيان خدمات تقنية المعلومات الدعم إلى وحدات الأعمال التي ستستخدم هذا البيان بالإضافة إلى أقسام تقنية المعلومات التي ستوفر خدمات تقنية المعلومات على المستوى الإستراتيجي، والتخطيطي، وكذلك على مستوى الإدارة التشغيلية، بمعنى أن هذا البيان يجب أن يُبْنَي أولاً على مستوى رفيع جداً بحيث يمكن لكل من الإدارة العليا وإدارة تقنية المعلومات على مستوى المدير التنفيذي للمعلومات أن يتخذوا في البداية قراراً حول أنواع العروض التي سيشملها البيان. فعلى سبيل المثال، قد تحتاج إحدى مؤسسات التجارة المالية إلى العديد من أدوات الوصول التي تساعدها في إتمام أعمالها التجارية. فأي مستثمر يبحث عن برامج خاصة باختيار سوق الأسهم، على سبيل المثال، يدرك أن هناك العديد والعديد من أدوات اختيار وتحليل الأسهم. على أية حال، يمكننا القول وبكل بساطة بأنه من غير المجدي لا من الناحية العملية ولا من الناحية الاقتصادية أن يتم إدراج كل أدوات التحليل هذه في بيان المؤسسة وجعلها متاحة لأي مستوى من المستويات الخاصة بمستخدم النظام. بل ينبغي على وحدات الأعمال وقسم تقنية المعلومات أن يقوموا بفحص تلك البدائل المختلفة، وأن يضعوا فقط البدائل المقبولة أو المتعارف عليها في بيان خدمات تقنية المعلومات لديهم.

يوضح الشكل التوضيحي (١٢-١) تلك العلاقة الخاصة ببيان خدمات تقنية المعلومات بين وحدات الأعمال والإدارة الخاصة بمزود خدمات تقنية المعلومات. وليس بالضرورة أن يعبر المثلث الظاهر على يسار الشكل عن كامل المؤسسة، فهو من الممكن أن يعبر عن قسم أو وحدة أعمال أو مجموعة تشغيلية مستقلة لها مطالبها وأنظمتها الخاصة بها. فضلاً عن أن هناك وحدة معينة لنظم وعمليات تشغيل تقنية المعلومات ستقوم عادة بدعم تلك الوحدة المستقلة للأعمال. الفكرة هنا هي أنه لا بد من أن يتم وضع الإستراتيجية الشاملة لبيان خدمات تقنية المعلومات على مستوى إستراتيجي من قبل الإدارة العليا لتقنية المعلومات والإدارة العليا للتشغيل والمالية. الأمر الذي سيؤدي إلى إيجاد قيود من المستوى الأعلى تعد بمثابة الأساس لبيان خدمات تقنية المعلومات ومحفظة الخدمات الخاصة بالمؤسسة.

إن بيـان الخدمة على المسـتوى الإسـتراتيجي يغطي عروضاً رفيعة المسـتوى لخدمات تقنيـة المعلومات مثـل الخصائص والخيارات الرئيسـية المتاحة من خـلال نظام تخطيط الموارد المؤسسـية Enterprise Resource Planning (ERP) والذي تم تطبيقه اسـتناداً إلى مـشروع اختيار وتطبيق البرمجيات الخاصة بأحـد الباعة. إن أي نظام خاص بتخطيط الموارد المؤسسية ERP يوفر العديد من الخيارات والميزات، ويحتاج إلى مستويات عالية من التدريب والوعي لكل من المستخدمين والعاملين بمرفق تقنية المعلومات لتحقيق الاستفادة المرجوة من الميزات الخاصة بالنظام. وسـنتطرق للحديث عن قضايا حوكمة نظم تخطيط الموارد المؤسسية ERP في الفصل الخامس عشر من هذا الكتاب. وسيتم تقديم نوع ERP الذي تم اختياره لأحد النظم الرفيعة المستوى في بيان الخدمة على مستوى إستراتيجي.

شكل توضيحي (١٢-١)

علاقات الأعمال الخاصة بخدمات تقنية المعلومات



ثم يـأتي بعد ذلك منظور إدارة التخطيـط (الإدارة التكتيكية) وهو ضروري لبناء أي بيان خدمات وتحقيق الترابط بين قسم تقنية المعلومات وإدارة عمليات التشغيل وإدارة عملاء وحدة الأعمال التابعين لها. فهي عملية مكونة من عدة خطوات وموضحة بالشكل (١٢-٢). وفي خطـوة أولى، يجب على إدارة تقنيـة المعلومات أن تنظر بتمعن إلى موارد تقنية المعلومات الموجودة لديها والعمل على إعادة تشـكيلها على أنها خدمات موجهة للمسـتخدمين. على سـبيل المثال، قد يكون لدى إحدى المؤسسـات بعـض التطبيقات الرئيسـية الخاصة بالمحاسبة والمالية، مثل دفتر الأسـتاذ العام والخاص بالإقفال في نهاية الشهر. هنا، ربما يكون من الضروري تسليط الضوء على عمليات التحليل الخاصة الأخرى ووصفها وتحديد المسـتخدمين المحتملين لها وإضافتها كسـجلات في بيان الخدمة. هذا سيحولها من مجرد عمليات تقنية إلى خدمات خاصة بالعملاء كما هو موضح في الشكل التوضيحي (١٢-٢).

وفي خطوة تالية، يجب أن تُحوَّل الخدمات التقنية الخاصة بالعملاء إلى عمليات محددة في الأعمال المؤسسـية. وتفرض هذه الخطوة على فريق تقنيـة المعلومات وفريق الأعمال الذهـاب إلى ما هو أبعد من مجـرد قائمة بالتطبيقات المنفذة لديهـم والتي يمكن وصفها في بيـان الخدمات. الفكرة هي أنه يجب تقديم المزيد من التفاصيل التي تسـمح بتمكين العمليـات الخاصة بالأعمال على نحـو أفضل. لذا يجب أن يحدد بيـان تقنية المعلومات هذه العمليات الخاصة بالأعمال على نحو أفضل كي تسمح للمستخدمين بأن يفهموا كيفية اختيار واستخدام تلك العمليات الخاصة بالأعمال. وقد تكون الإجراءات الخاصة بالتعيينات الجديدة في إحدى وحـدات المنظمة مثال على أحد أنواع العمليات التي يمكن إضافتها إلى بيان كهذا. فالوحدة التقليدية في المؤسسـة لا تسـتقطب العديد من الأشخاص الجدد على نحـو منتظم، غير أن هناك عمليـات خاصة لازمة لمثل هذا الموظف الجديد، والتي تتضمن فحص المعلومات الأساسية والعروض الخاصة بخطة الاستحقاقات والتقاعد والامتثال لمدونة قواعد السـلوك وما هو أكثر من ذلك بكثير. فبيان تقنية المعلومات سـيقود المسـتخدمين لتلك الخدمات الضرورية وسيوجههم إلى تحقيق الامتثال.

محتوى بيان خدمات تقنية المعلومات وسماته:

تعد بيانات خدمات تقنية المعلومات من الإصدارات الشائعة في العديد من المؤسسات اليوم. ولكن ينبغي أن تكون هذه البيانات أكثر بكثير من مجرد قوائم طويلة تحتوي على أسماء ملفات التطبيقات التي تكون أشبه بما يمكن أن نجده في قائمة أحد مجلدات أنظمة التشغيل المعتمدة على النوافذ. لذا يجب أن يتم تصميم أنواع الخدمات المقدمة لتتناسب مع المنظمة وأهدافها. إن البحث في الويب عن مؤسسات أخرى قد يزودنا بالعديد من الأمثلة لما يجب أن يظهر به سجل البيانات الخاص بخدمات تقنية المعلومات، ومع أن العديد من مصادر شبكة الإنترنت تقوم بوصف منتجات البائع الذي يقوم بتسويق الحلول الخاصة به، فإنه من ناحية أخرى نجد أن بيان الخدمة النموذجي يبدأ صفحة رئيسية على الإنترنت تخص قسم تقنية المعلومات التابع للمؤسسة، حيث يلفت انتباه الأعضاء المصرح لهم بالدخول إليه من بين مجتمع المستخدمين الخاص بالمؤسسة إلى خدمات تقنية المعلومات المتاحة.

شكل توضيحي (١٢-٢)

عناصر بيان خدمات تقنية المعلومات



وعـلى الرُغـم من أن المؤلف هنا غـير محترف في تصميم مواقع الإنترنت، فإن الشـكل التوضيحي (١٢-٣) يعرض مثالاً على الواجهة الرسـومية الأمامية أو الصفحة الرئيسية لبيان الخدمـات الخاص بالشركة العالمية لمنتجات الحاسـب (Global Computer Products) التي تمت الإشارة إليها في فصول أخرى من هذا الكتاب. فبعد أن يقوم الموظف أو غيره من أصحاب المصلحة المصرح لهم بتسـجيل الدخول باستخدام معرف فريد محدد وكلمة مرور خاصة به، فإنه سـيرى هذا النوع من الصفحات الرئيسـية، والتي تسرد المجالات المختلفة المتاحة لدعم النظم والتطبيقات الخاصة بها. فعلى سبيل المثال، قد يقوم المستخدم المصرح لـه بعد ذلك بالنقر على رابط خدمـات مراقبة التطبيقـات applications monitoring services. وقـد تكون هذه عبـارة عن أدوات خاصة لتحسـين تطبيقات أخرى مخصصة للمستخدمين، حيث يشير الرقم (٥) بعد الرابط Application Services إلى عدد التطبيقات الأخرى المتاحة المتعلقة بهذه الفئة. ومع عدم مشاهدة تلك التطبيقات هنا، فإن النقر على الرابط سيعرض لنا قائمة بتلك التطبيقات الخمسة.

يمكن أيضاً عرض مجموعة من الخيارات الإضافية على أنها جزء من تلك العينة لصفحة بيان الخدمات مع روابط لصفحات أخرى تشمل:

- **طلبـات الخدمـة Service requests:** وسـتكون هذه عبارة عن بيـان لعرض طلبات المستخدمين المتعلقة بالحصول على بعض التطبيقات الجديدة والخدمات الأخرى لتقنية المعلومات.
- **حالة تذاكر المشاكل Problem ticket status:** يقوم مستخدمو تقنية المعلومات الذين يواجهون مشـاكل مع أي نوع من أنواع تطبيقات أو خدمـات تقنية المعلومات بتعبئة نوع من أنواع الوثائق الخاصة بتذكرة المشـاكل، وقد سـبق الحديث عنها على أنها جزء من آيتل في الفصل السادس من هذا الكتاب.
- **تاريخ التدريب Training history:** يجب أن تقدم الصفحة الرئيسية تقريراً عن حالة البرامج التدريبية المتاحة للمستخدمين حسب معرف المستخدم User ID.
- **روابـط الاتصـال بإدارة تقنية المعلومـات:** من الممكن أن تكون روابـط عامة لتقديم المساعدة.

ولأن أي بيــان خدمات كهذا لن يتمكن من تغطية جميع طلبات المســتخدمين، فلا بد أن يكون لدى المؤسســة إحــدى العمليات المعمول بها والخاصة بالتذاكر حيث يســتطيع المســتخدم أن يقــوم بكلٍ من تقديم الطلبات الخاصة وفحــص حالة أي تذاكر تم تقديمها. إضافة إلى ذلك فإنه يجب الاحتفاظ بســجلات دقيقة عن النشاطات التدريبية. ومن المهم توضيح أن هناك موظفين محددين قد تلقوا تدريبات في تطبيقات رئيســية وأنهم قد أتموا متطلبات تلك التدريبات.

ومن الممكن أيضاً تنظيم بيان الخدمات من خلال مجموعات من اللوحات الخاصة التي تحتوي على روابط للتطبيقات والخدمات المتاحة للموظف المســتخدم. بحيث تكون تلك القائمة من الروابط مرنة وتعتمد على الصلاحيات الخاصة بدخول المســتخدمين. فالمشرف في القطاع التسويقي مثلاً يستطيع أن يرى فقط الروابط الخاصة بالتطبيقات المصرح له أو لها بالوصول إليها. في حين أن لوحات أخرى تقدم للمستخدم معلومات عن أرقام الاتصال بالدعــم الفني وأهم الأخبار المتعلقة بالنظم ومعلومات خاصة بالفيروســات وحالة الأمن. وقــد تــم الحديث عن قضايا الأمــن الخاصة بتقنية المعلومات في الفصــل العاشر من هذا الكتــاب، كما يجب أن تكون هنــاك نظم معمول بها لإخطار جميع المســتخدمين بالوضع الحالي للقضايا المتعلقة بالفيروسات والأمن.

تحتوي اللوحة الموجودة في الجانب الأيسر من هذا المثال للصفحة الرئيسية على قائمة من الخدمات التي ســتكون متاحة للمستخدم اعتماداً على صلاحيات وحقوق الوصول الخاصة بهوية المســتخدم أو المســتخدمة. وتكون هذه القائمة في العادة نوعــاً من أنواع الطلبات الخاصة بالتطبيقات التي لا تُدرج ضمن النشــاطات اليومية الاعتيادية للمستخدمين ولكن قد تكون ضرورية لمتطلبات خاصة.

قد يكون بيــان خدمات تقنية المعلومات بمثابة أداة هامة لتنظيم، وحتى التحكم نوعاً ما، بعمليات الوصول إلى موارد تقنية المعلومات الخاصة بالمؤسســة. لذلك يجب تشــجيع كل من كبار المديرين ووحدات تقنية المعلومات التابعين لها على تطبيق واستخدام بيانات فعالة للخدمات والتي سوف تسمح لجميع أصحاب المصلحة المعنيين في المؤسسة باستخدام موارد تقنية المعلومات داخل حدود مسؤولياتهم بشكل فعال.

إدارة بيان خدمات تقنية المعلومات:

ربمـا يكون اهتمام بائعي تقنية المعلومات والإعـلام التقني المرتبط بتقنية المعلومات هو السـبب وراء جعل بيانات خدمات تقنية المعلومات أحد الأشياء العصرية التي يمكن تطبيقها بالنسـبة للعديد من المؤسسـات خلال السـنوات الأخيرة. من ناحية أخرى فإن بـذل الوقـت والموارد عـلى تطبيق كهذا لن يعـود بقيمة كبيرة على المؤسسـة ما لم يتم تخطيط، وتنفيذ، وإدارة الجهود بشكل فعال في أرجاء المؤسسة كافة. فعمليات إدارة بيان الخدمـات تمنح تقنية المعلومات القدرة على التحكم بالمبادرات الداخلية لتطوير وتقديم الخدمات ودعمها عند تأسـيس الشراكة مع المسـتهلكين الذين سيحصلون على الخدمات المتفق عليها بمستويات وأسـعار متوقعة. وتتضمن فوائد الإدارة الفعالة لخدمات تقنية المعلومات ما يلي:

- إيجاد ثقافة تقديم خدمة والتي أسـهمت في تغيـير النظرة التي ننظرها لإدارة تقنية المعلومات من مجرد قسم من أقسام الشركة إلى أن تكون مزود خدمات.

- توفير مصدر للمعلومات الموثوقة لإدارة استثمارات تقنية المعلومات على نحو أفضل.

- رفع مسـتوى الرضا لدى العملاء عن طريق السماح لهم باختيار المستويات الصحيحة لخدمات تقنية المعلومات التي تلبي رغباتهم.

شكل توضيحي (١٢-٣)

الصفحة الرئيسية لبيان خدمات الشركة العالمية لمنتجات الحاسب

Global Computer Products

Information Technology Division

IT Service Catalog Home Page

User-ID:	Password:

FIND a Service: ________________. A–Z Listing | Recently Added | Print Version

- Application Services (5)
  Application Monitoring Services, Call Center Management (Operator Services), Custom Application Development
- Communication/Collaboration Services (23)
  ActiveSync Wireless Messaging Services (iPhone, Windows Pocket PC, Palm, smartphone), BlackBerry Wireless Messaging
- Connectivity Services (10)
  Paging Network Support, Cable Management—Inter/Intra Building Connectivity, Consolidated Network Monitor
- Enterprise Applications IT Support (3)
  Business Intelligence Services, Enterprise Application Services, Enterprise Directory Services
- Hosting Services (7)
  Co-Location Services, Database Hosting Services, Google Search Engine Service, Mainframe Hosting Services
- Infrastructure Services (13)
  Active Directory Development and Testing Services, Active Directory Management and Operations Services, Desktop
- Professional Services (5)
  Consulting Services, General IT Security Services, IT System Security Assessment and Authorization Relationships
- Support Services (10)
  Deskside Support Services, eDiscovery Services, Media Sanitization Service, Messaging and Infrastructure Support
- Training Services (3)
  Custom IT Training, IT Training Facilitation (Classroom Rental), IT Training

Please contact the Global Computer Products IT Service Desk if you need any additional information about services in this catalog.

ينبغـــي على إدارات تقنيـــة المعلومات أن تقوم بتعبئة مواردهـــا، بموافقة الإدارة العليا، لبنـــاء وصيانة بيـــان خدمات تقنية المعلومات الذي يحتوي عـــلى معلومات دقيقة عن كل خدمة من الخدمات الموجودة وعن تلك التي تم إعدادها لتعمل بشكل تشغيلي.

إن الجهد المبذول لتطوير بيان خدمات مثل هذا ســيعود بفوائد كبيرة على الصعيدين الداخلي والخارجي. فعـــلى الصعيد الداخلي، ينبغي على إدارات تقنية المعلومات أن تقوم بتطوير وإطلاق خدماتها بناء على المتطلبات المستمدة من إستراتيجيات الأعمال في المؤسسة. أما على الصعيد الخارجي، فيستطيع عملاء تقنية المعلومات فهم توجهات تقنية المعلومات وطلب الخدمات ومستوى الخدمة التي تستطيع أن تقدمها لهم تقنية المعلومات.

تتضمن الخطوات الرئيســـية للقيام بإنشاء بيان خدمات فعال لتقنية المعلومات وإدارة تلك العمليات بشكل فعال، ما يلي:

- **توثيـــق تعريف خدمة تقنية المعلومات:** يعـــد التوصل إلى توافق ينتهي بتوثيق تعريف خدمـــات تقنية المعلومات بمثابة الخطوة الأولى، وربما تكون الأكثر صعوبة في هذا المقام. فالسؤال هنا موجه لكل من إدارة تقنية المعلومات وإدارة المستخدمين "ما المقصود بخدمة تقنية المعلومات؟" إن الإجابة عن هذا الســـؤال ليســـت بالأمر السهل، ومن المحتمل أن تكون إدارة تقنية المعلومات قد بذلت الكثير من الوقت قبل الوصول إلى تعريف محدد وواضح للخدمة. إلا أن الإطار آيتل الذي تم تقديمه في الفصل الســـادس من هذا الكتاب يقدم تعريفاً جيداً واضحاً للخدمة وهو أن: "الخدمة هي وســـيلة لتقديم قيمة للعملاء من خلال تسهيل النتائج التي يريد أن يحققها المستهلك دون تحمل التكلفة أو المخاطر".

ومـــن الآثـــار التي يمكن أن تنتج عـــن العمليات الفعالة لإدارة بيـــان الخدمات إمكانية مراقبـــة وفهم التغيرات التي تحدث عـــلى متطلبات وخدمات الأعمال. لذا يجب أن تتلقى إدارة تقنيـــة المعلومـــات معلومات عن الأعمال على أنها مدخـــلات من وحدات الأعمال في المؤسســـة حتى تتمكن من وضع الخطط الإســـتراتيجية والمالية لتقنية المعلومات. اعتماداً على المتطلبات الحالية والمستقبلية الموجودة في محفظة الخدمات الحالية لتقنية المعلومات. وهذا سيسمح لبيان الخدمات أن يصف بدقة جميع الخدمات التي سيكون هناك حاجة إلى نشرها. وقد تتضمن هذه المعلومات التفاصيل المتفق عليها بخصوص مســـتويات الخدمة

وعلى مسائل أخرى كالوقت المناسب للتسويق والتغيرات التي طرأت على العمليات الرئيسية للأعمال المعتمدة على خدمات تقنية المعلومات.

كما سيحتوي تعريف الخدمات أيضاً على معلومات تتعلق بوحدات الأعمال التي يمكنها أن تطلب الخدمة، وعن أصحاب الأعمال ومدير الخدمة الذي سيقوم بالتصديق على طلبات الخدمات. كما يجب أن تشتمل الوثيقة أيضاً على تفصيلات وحالات جميع الخدمات التشغيلية، وأيضاً تلك التي تم نقلها إلى الإنتاجية.

- **بناء محتويات البيان:** بمجرد أن يتم توثيق تعريف الخدمات وكل المعلومات المرتبطة بها، يمكن لتقنية المعلومات إنشاء محتوى بيان الخدمات الخاص بها. وهو عبارة عن نشاط يتضمن كيفية تنظيم عروض الخدمات وتزويد المستهلك بكل التفاصيل المتفق عليها.

وربما تنتج بعض الصعوبات غير المتوقعة أثناء بناء المحتوى جراء بعض التعريفات المعقدة للخدمات. يجب أن نتذكر دائماً أن "الخدمة" قد تتضمن أنشطة أخرى، مثل المكونات الرئيسية للبنية التقنية الرئيسية بما فيها من معدات وتطبيقات وشبكات وبيانات. ومن الممكن أن يكون ذلك مجدياً في تحديد التسلسل الهرمي للخدمات الموجودة بداخل البيان من خلال إعداد وتجميع أنواع الخدمات المسجلة، متضمناً ذلك خدمات الأعمال والدعم الفني والبنى التحتية والشبكات والتطبيقات. إن سؤال العملاء عن الخدمات التي سيقومون باستخدامها وعن الكيفية التي ستسهم بها هذه الخدمات في دعم عمليات الأعمال الخاصة بهم، يمكن اعتباره أحد الوسائل البسيطة للقيام بهذا النشاط الخاص ببناء محتوى البيان. إن تطوير وملء ما يعرف بقالب تعريف خدمات تقنية المعلومات والموضح في الشكل التوضيحي (١٢-٤) قد يكون هو نقطة البداية الرئيسية لهذه العملية. فملء تلك القوالب المعرفة مسبقاً لتعريف الخدمات ومن ثم توزيعها بين أصحاب المصلحة الرئيسيين لمراجعتها والموافقة عليها سيسهل كثيراً من هذه المهمة.

- **إنشاء نوافذ لخدمات الأعمال:** يعد وجود حاجة لفهم طرق عرض خدمات الأعمال جزءاً أساسياً من عملية تطوير بيان خدمات تقنية المعلومات، إذ تشتمل طرق العرض هذه على تفاصيل كثيرة تتعلق بجميع خدمات تقنية المعلومات المقدمة للعملاء، كما تحتوي أيضاً على توصيفات وتفاصيل يستطيع أن يفهمها العميل، وتحتوي كذلك على العلاقات

الموجودة بين وحدات وعمليات الأعمال المعتمدة على خدمات تقنية المعلومات. فشاشة خدمة الأعمال هي نافذة العميل على بيان خدمات تقنية المعلومات كما أنها تسهم في تطوير عملية أكثر فاعلية لإدارة مستوى الخدمة.

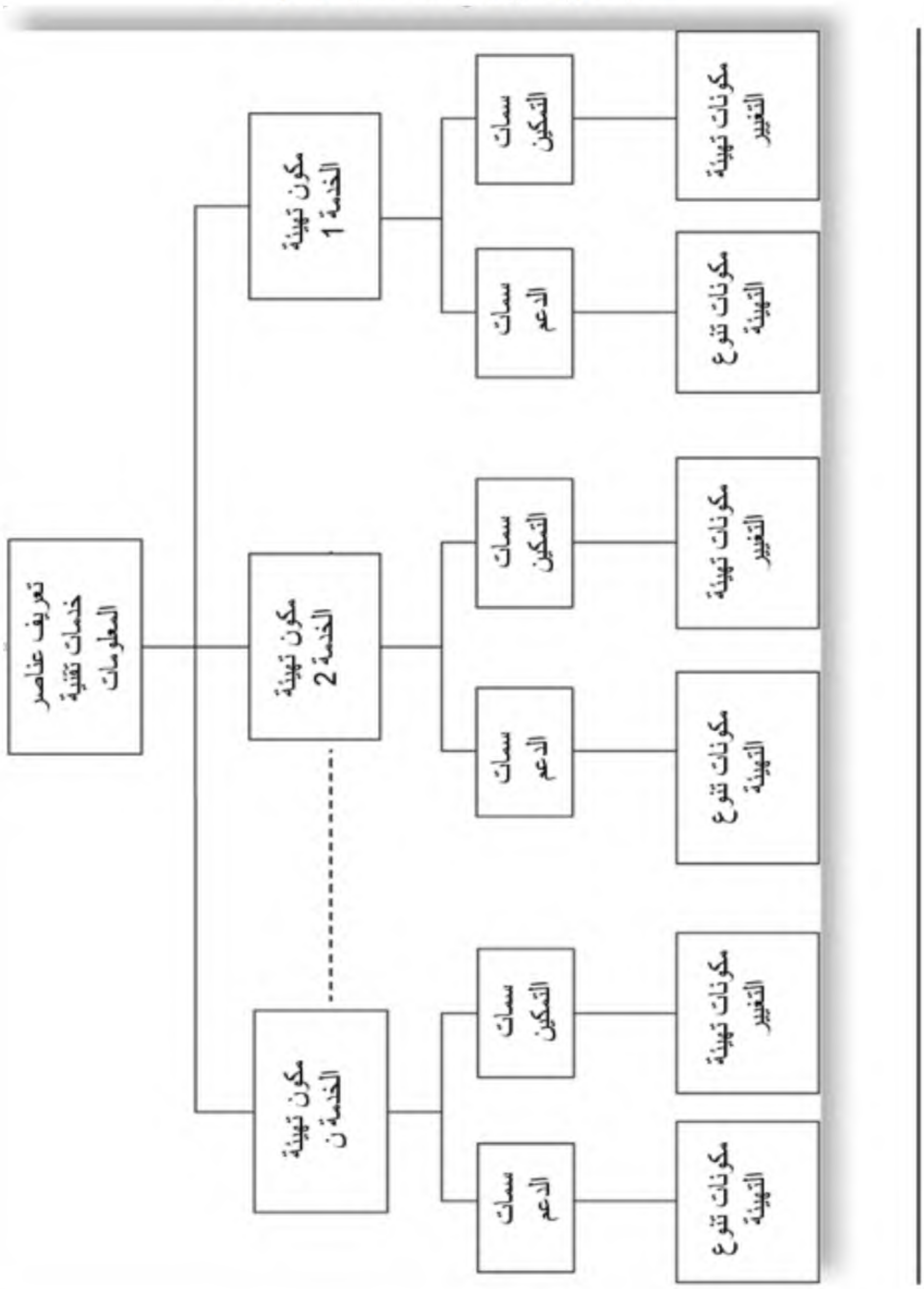
قد تساعد الحلول التقنية المستخدمة في إنتاج طرق لعرض خدمات الأعمال، الأمر الذي يسمح لتقنية المعلومات باتخاذ قرارات حاسمة حول الخدمات التي يتم طلبها وعدد المرات التي تُطلب فيها ومعرفة احتمالية دمج بعض الخيارات التي من الممكن أن تكون مرتبطة بالخدمة ومستويات الخدمة التي من الممكن أن تُطلب.

- **إنشاء طرق لعرض الخدمات التقنية:** نظراً لهيكلة خدمات تقنية المعلومات، فإن هناك العديد من خدمات الدعم الفني تكون غير مرئية بالمرة لمستخدمي وعملاء تقنية المعلومات، والتي يجب أن تبقى كذلك، إلا أنها أساسية وضرورية لتقديم خدمات تقنية المعلومات. يختلف بيان الخدمات التقني عن منظور خدمات الأعمال، فهو يحتوي على تفاصيل جميع خدمات تقنية المعلومات التي تم تقديمها للعميل إلى جانب علاقاتها بخدمات الدعم، والمكونات، وعناصر التهيئة اللازمة لدعم تقديم الخدمات للأعمال.

إن العديد من المؤسسات تقرر الاحتفاظ ببيان خدمات أعمال فقط أو بيان خدمات تقنية فقط. على أية حال، فإن الوضع المفضل الذي تم تبنيه من قبل المؤسسات الأكثر نضوجاً هو الاحتفاظ بكلا الجانبين بداخل بيان خدمات واحد يعتمد على الأدوار. فهو يسمح لمستخدمين مختلفين من الوصول إلى شاشة الأعمال أو شاشة الدعم التقني أو الشاشتين معاً وفقاً لصلاحياتهما.

شكل توضيحي (١٢-٤)

قالب تعريف بيان خدمات تقنية المعلومات



• **نشر الخدمات النشطة في بيان الخدمات:** خطوة أخيرة ومهمة إدارية هامة للغاية، يجب أن تقــوم إدارة تقنية المعلومات بنشر بيــان الخدمات الخاصة بها لعملائها. ويعد ضبط وتطويــر واجهة تعتمد على الويب تســمح بالوصول إلى الخدمــات المعروضة هو الحل الطبيعي في هذه الحالة. ويوضح الشكل التوضيحي (١٢-٣) مثل هذه الصفحة الرئيسية لبيان خدمات منشور على شبكة الويب.

إن إجراء الدراســات المتعلقة بإمكانية وســهولة وفحص الأداء بشــكل مسبق يعد من الممارسات الجيدة في هذه الحالة. آخذين بعين الاعتبار اختلاف أنواع ومستويات الموظفين التــي يمكــن أن تكون موجودة بداخل هيكلة المؤسســة. ومن المهم أيضــاً النظر في أدوار وصلاحيات المســتخدمين في وحدات الأعمال الخاصة بهم وفي السياسات الخاصة بالمنظمة. لذا يجب أن يُبني بيان الخدمات بشكل يسمح للمستخدمين بطلب الخدمات التي يرغبون فيها بسهولة لهم وبالنيابة عن الآخرين. كما يجب أن يحتوي البيان على تسهيلات للموافقة عــلى طلبات الخدمات المقدمة. يمكن لهذه الأمور الخاصة ببيان الخدمات أن تجعل حياة إدارة تقنية المعلومات أسهل بكثير في التمهيد لتقديم نظام جديد.

قبل نشر أي بيان لخدمات تقنية المعلومات، ينبغي على كل من قسم تقنية المعلومات والمســتخدمين الأساســيين أن يقومــوا بفحص جميع الأمــور المتعلقة بالمنتج. وهو أشــبه بالفحوصات الضرورية المتعلقة بضمان جودة أي مبادرة جديدة. إن فحص بيان الخدمات يعنــي ضمنياً فحص الوظائف التقنيــة التي تعد الهدف الطبيعي مــن الخدمة إضافة إلى فحص أكثر لمدى إمكانية الاســتخدام الشــخصي. فكلا الأمرين هــام لتحقيق النجاح الكلي وتبني أي بيان لخدمات تقنية المعلومات.

إن بيــان خدمات تقنية المعلومــات عبارة عن عملية إدارية هامة مســؤولة عن إنتاج ووصــف لجميع خدمات تقنية المعلومات والاحتفاظ به. كــما أن المعلومات الموجودة في بيان الخدمات المخطط له والمعد على نحو جيد ينبغي أن تعد لتعمل بشــكل تشغيلي كما ينبغــي أن تضمن أن المعلومات الخاصــة بخدمات تقنية المعلومــات المتفق عليها متاحة بشكل واسع لأولئك الذين لهم حق الوصول إلى تلك الخدمات.

تســتطيع التقنية أن تلعب دوراً هاماً في تحســين عملية إدارة بيان الخدمات من خلال أتمتة الأنشــطة الفعلية للعملية وبناء عروض خدمات من خلال بنية وحدة الأعمال، وأيضاً مــن خلال الوصول إلى المخرجات الناتجة من عمليــات أخرى مرتبطة ببيان الخدمات. إن بيان الخدمات الفعال لأعمال تقنية المعلومات والمدار بشكل جيد يعد من العناصر الفعالة للحوكمة الرشيدة لتقنية المعلومات.

الجزء الرابع

بناء أنظمة حوكمة تقنية معلومات فعالة ومراقبتها

الفصل الثالث عشر
أهمية البنية الموجهة نحو خدمات تقنية المعلومات لنظم حوكمة تقنية المعلومات

يعلـم المحترفون الذين عملوا مع نظم وتطبيقات تقنية المعلومات على مر السـنين أن الأسـاليب والتقنيـات المتبعة في عالم تقنيـة المعلومات دائمة التغـير والتطور. ففي أغلب الأحيان نرى أن المفهوم الذي كان يعتبر جديداً وسـاخناً منذ سـنوات قليلة فقط سرعان ما يندثر ويسـتبدل بمفهـوم آخر جديد ومختلف كلياً. ونرى في حـالات أخرى أنه سرعان ما تتطـور وتتحـول المفاهيم التي كانت في يوم من الأيام عبـارة عن مفاهيم متقدمة جداً أو حتى غريبة بعض الشيء إلى ممارسـات اعتيادية ومقبولـة. إن تجهيزات وإعدادات نظام الحاسبات القائم على الخادم - العميل يعد واحداً من الأمثلة على هذا النوع من الممارسات. فربما كانت تلك الإعدادات في منتصف تسـعينيات القرن الماضي تعد من المفاهيم الجديدة والمختلفة، إلا أنها الآن أصبحت اللغة المعيارية الموحدة في تقنية المعلومات. نجد أيضاً أن إدارة تطبيقات تقنية المعلومات من خلال البنى الموجهة نحو الخدمات Service Oriented Architecture (SOA) تعد هي الأخرى من المفاهيم الجديدة نسبياً والتي ستصبح قريباً جزءاً من اللغة القياسية الموحدة في تقنية المعلومات. إننا نستخدم هنا الاختصار SOA مع أن هناك آخرين يستخدمون أحياناً الاختصار Software as a Service (SaaS) (البرمجيات كخدمة) للدلالة على المفهوم نفسه. فكلا الاختصارين يعني الشيء نفسه، إلا أننا نستخدم الاختصار SOA خلال هذه الفصول خلال شرحنا لهذا المفهوم.

إن البنيـة الموجهـة نحو الخدمـات SOA هي إحدى وسـائل نظم تقنيـة المعلومات التـي يتم مـن خلالها تجزئة الوحـدات الإجرائية المنطقية الخاصـة بتطبيقات الأعمال أو الوظائف الفردية وتقديمها خدمات للتطبيقات الخاصة بـالمسـتهلكين أو المسـتخدمين. إن الفكرة الأساسية هنا هي أن تكون خدمات تقنية المعلومات التي يتم تقديمها فعلياً بعيدة ومستقلة كلياً عن التنفيذ الفعلي للتطبيق أو النظام. الأمر الذي يجعل مطوري نظم تقنية المعلومـات قادرين على بناء وتكوين تطبيقات جديدة من خلال اختيار وتجميع المكونات

المختلفة لتقنية المعلومات. وهذا أشــبه بالطريقة التي يقوم بها الطفل ببناء شــكل جديد باستخدام قطع مختلفة من لعبة الليغو[1] LEGO.

ســيقوم هذا الفصــل بتقديم المفاهيــم الخاصة بالبنية الموجهة نحــو الخدمات SOA لنظم وتطبيقات تقنية المعلومات، كما سيناقش أيضاً قضايا الرقابة الداخلية وحوكمة تقنية المعلومات الخاصة بتطوير تطبيقات تقنية المعلومات وعملياتها التشغيلية باستخدام هذه التقنية. يعد مفهوم البنية الموجهة نحو الخدمات SOA من المفاهيم التي تتطور بفاعلية وسرعــة في مجال تطوير وتنفيــذ التطبيقات الخاصة بتقنية المعلومــات. فعندما يتحدث العاملــون بــإدارة تقنية المعلومات في المؤسســة عن البنية الموجهة نحــو الخدمات SOA ويقومون باستخدام هذا المصطلح كما لو كان تعبيراً جديداً ومؤثراً، فإنه يجب على مديري الأعمال أن يتمتعوا بمســتوى فهم عام فيما يخص هــذا المفهوم، وكذلك الضوابط الداخلية والمفاهيم المحيطة بتطبيقات البنية الموجهة نحو الخدمات SOA.

تطبيقات البنيــة الموجهة نحو الخدمة (SOA) وتطبيقــات تقنية المعلومات المدفوعة بالخدمة:

يقــوم بائعو الأجهزة والبرمجيــات غالباً وكذلك مطــورو تطبيقات البرمجيــات العالية المســتوى باستخدام مصطلحات متشــابهة ولكنها مختلفة قليلاً أثناء حديثهم عن مفاهيم البنية الموجهة نحو الخدمات SOA. فربما نســمع تعبيرات كالهياكل الموجهة نحو الخدمة Service-Oriented Architectures والتصميم الموجه نحو الخدمة Service-Oriented Design والتصميــم الموجه نحو الهــدف Object-Oriented Design أثناء الحديث عن خصائص بعــض التطبيقات الجديدة لتقنيــة المعلومات. فهذه التعبيرات تبدو متشــابهة وتشير عموماً إلى الأساليب والطرق نفسها التي يتم من خلالها بناء وتطوير تطبيقات تقنية المعلومــات ونشرها في عالمنا اليــوم الموجه نحو الإنترنت. وســنقوم عموماً في هذا الفصل باســتخدام مصطلح البنية الموجهة نحــو الخدمــات Service-Oriented Architecture للإشــارة إلى هذا المفهوم على الرغم من أنه قد يختلف علماء الحاسب حول بعض تفاصيل المصطلح.

إن البنيــة الموجهة نحو الخدمات SOA عبارة عن نمط هيكلي لتقنية المعلومات يهدف إلى تحقيق التقارن أو الارتباط الضعيف loose coupling بين وكلاء البرمجيات. وللمساعدة في توضيح التعريفات، يصف لنا هذا التقارن الضعيف loose coupling كيف يمكن للنظم المتعددة في الحاســب الآلي، حتى وإن كانت تلك النظم تســتخدم تقنيات غير متوافقة، أن يرتبط بعضها ببعض لتقوم بتنفيذ المعاملات المطلوبة بغض النظر عن المعدات والبرمجيات والمكونات الوظيفية الأخرى الخاصة بتلك النظم. فعلى سبيل المثال، تعتبر الحاسبات الآلية المســتخدمة في الشــبكة عبارة عن نظم ضعيفة الترابط loosely coupled systems حيث يمكــن لجهــاز العميل أن يقوم بطلــب بيانات من جهاز الخادم حتى لــو كان النظامان أو الجهازان يعمل كل منهما بشكل مستقل عن الآخر.

تسمح البنية الموجهة نحو الخدمات SOA بتحقيق التشغيل البيني أو التبادلي بين النظم ولغات البرمجة المختلفة لتقنية المعلومات. موفرةً بذلك أساس التكامل بين التطبيقات التي تعمــل على منصات مختلفة من خلال الرســائل عبر وصلات شــبكة الاتصــالات. يتم بناء البرمجيات باتباع كل من المعايير المشــتركة والمعايير الخاصة بالصناعة والتي هي عبارة عن مكونات محببة (مقســمة) ومعيارية. إن الخدمة هي وحدة من وحدات الأعمال التي تم إنجازها بواســطة مقدم الخدمات لتحقيق النتائج النهائية المرجوة لمســتهلك الخدمة. إذ إن كلاً من مقدم ومســتهلك الخدمة ما هو إلا أدوار يقوم بها وكلاء البرمجيات بالنيابة عن أصحابها.

على الرغم من أن هذا الوصف قد يبدو للبعض تجريدياً بشكل كبير، فإن مصطلح البنية الموجهة نحو الخدمات SOA ليس بذلك المفهوم الصعب. فأســطوانات الموسيقا الموجودة في منازلنا وكذلك مشــغلات الأقراص المدمجة تعتبر مثــالاً على مفاهيم البنية الموجهة نحو الخدمات SOA. فإذا كنت على سبيل المثال ترغب في تشغيل أحد الأقراص المدمجة، فإنك تقوم بوضع القرص الذي تريده في مشــغل الأقراص لتقوم الوحدة الصوتية بتشــغيله لك. فمشــغل الأقراص في هذه الحالة يقوم بتقديم خدمة تشــغيل الأقراص الموسيقية المدمجة. وعند الانتهاء من ســماع القرص، يمكنك اســتبداله بقرص موســيقي مدمج آخر لســماعه. يمكنك أيضاً تشــغيل القرص الموسيقي نفسه باســتخدام مشغل أقراص محمول أو المشغل

الموجود بسيارتك الخاصة. فكلاهما يقوم بتقديم خدمة تشغيل الأقراص المدمجة نفسها. ولكن قد تختلف جودة الخدمة بسبب اختلاف الأنظمة الصوتية الموضوعة في كل منهما. وقد تؤدي نتائج خدمة تشغيل الأقراص الموسيقية إلى تغيير حالة المستهلك الذي يستمع إلى الموسيقا. فقد تتسبب في تغيير المزاج من مكتئب إلى سعيد. فنحن عملاء الخدمة Service Client ومشغل الأقراص هو مقدم الخدمة Service Provider وتقوم مكتبة الأقراص المادية الموجودة بدور الوسيط للخدمة Service Broker.

تماماً كما هو الحال بالنسبة لمشغل الأقراص الذي يقدم لنا الموسيقا المسجلة مسبقاً، فإن السبب وراء رغبتنا بوجود شخص آخر يقدم لنا الخدمات أو ينجز لنا الأعمال هو أنهم جميعاً يملكون مصادر مختلفة وخبراء مختصين. ويكون استهلاك الخدمة في العادة أقل تكلفة وأكثر فاعلية من أن نقوم بإنجاز الأعمال بأنفسنا. فمعظمنا يعلم بأننا لسنا أذكياء بما يكفي لنكون خبراء في كل شيء. والقاعدة نفسها تُطبق على بناء نظم البرمجيات.

ويقود هذا المفهوم الخاص باستخدام الخدمة الموسيقية لمشغل أقراص شخصي من مكتبة أقراص موسيقية إلى مفاهيم البنية الموجهة نحو الخدمات SOA. حيث تعتبر الخدمة هي اللبنة الأساسية لهذه البنية SOA، وأنها وسيلة للوصول إلى إمكانيات وقدرات أعمال قابلة للتكرار، ويتم تنظيمها لتكون واجهات برمجية بسيطة متاحة لجميع مزودي ومستهلكي الخدمة. يعرض لنا الشكل التوضيحي (١٣-١) هذا المفهوم الرئيسي الخاص بتكوين البنية الموجهة نحو الخدمات SOA، كما يعرض الشكل الآلية التي يقوم من خلالها العميل أو طالب الخدمة بطلب الخدمات من المقدم أو المجمع للخدمات من خلال وجود دليل أو بيان خاص بعروض الخدمات المتاحة لديهم. حيث سيقوم هذا البيان بسحب طلب الخدمة من أي مزود خدمة من بين العديد من مزودي الخدمات، وإعادة تلك الخدمة إلى طالب الخدمة ومن ثم إلى مزود الخدمة. إن مبدأ كل من بيانات الخدمات التي تم الحديث عنها في الفصل الثاني عشر من هذا الكتاب والبنية الموجهة نحو الخدمات SOA هو أن يتم تبني واستخدام إحدى بيانات الخدمات المتعارف عليها لتقديم الخدمات المطلوبة من تقنية المعلومات.

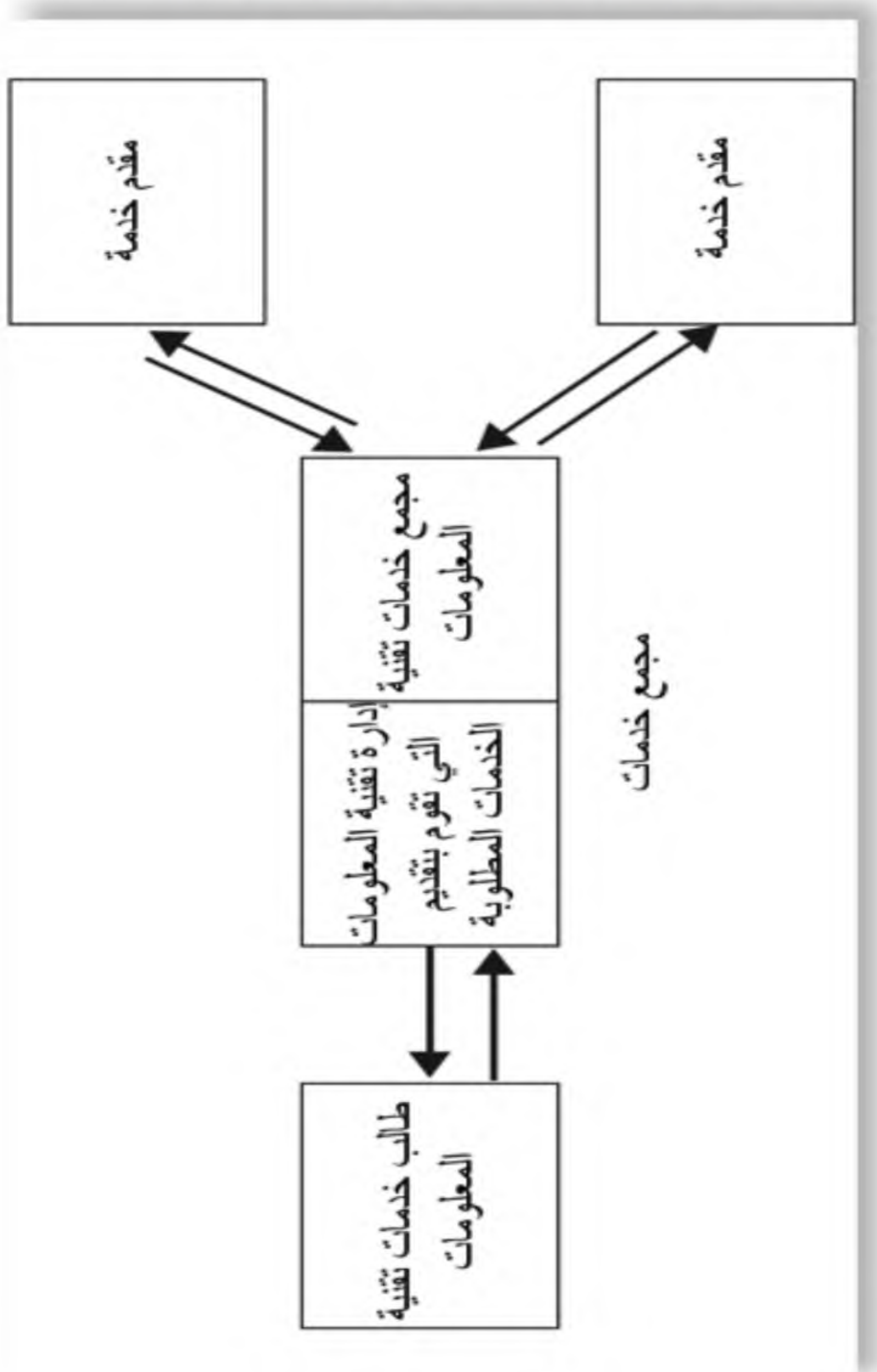
ولـكي تكون البنية الموجهة نحو الخدمات SOA أكثر فاعلية، فهناك حاجة إلى أن يكون لدى جميع مستخدمي نظم وخدمات تقنية المعلومات فهم واضح لمصطلح الخدمة. والأكثر أهمية في بعض الأحيان، هو الحاجة الفعلية لإدارة تقنية المعلومات لفهم ما يعنيه مصطلح الخدمة عندما تحاول القيام بتقديم خدمات تقنية المعلومات بدلاً من قيامها بتقديم النظم والعمليـات التقليدية الجديدة. فخدمة تقنية المعلومـات IT Service عبارة عن وظيفة معرفة جيداً وقائمة بذاتها ولا تعتمد على سـياق أو حالة الخدمات الأخرى. تعد الخدمات بمثابـة وحدات البناء بالنسـبة للبنية الموجهة نحو الخدمـات SOA والتي يمكن اختيارها وربطها معاً لعمل خدمات أخرى أو تجمعيها في تسلسل معين لإنشاء عمليات أخرى.

يتم تنظيم الخدمات في البنية الموجهة نحو الخدمات SOA بداخل ما يسمى بالسجل، وفيه يمكن جمع خدمات منفصلة لتشكيل تطبيقات مركبة منها، ومن ثم يتم تركيب بعضها مع بعض فيما يسـمى مخطط البنية الموجهة نحو الخدمات SOA blueprint. وبشـكل عـام تتعرض إدارة تقنيـة المعلومات إلى متاعـب متعلقة بالبنية الموجهـة نحو الخدمات SOA عندما تقوم بتقييم مجمل الضوابط العامة في المؤسسة الخاصة بها ومراجعة ضوابط محـددة في التطبيقـات. وعلى الرغم من أننا لا نهدف هنـا إلى تحويل القارئ إلى عَالِم في الحاسب الآلي أو مطور برمجيات، فإن هناك العديد من المفاهيم الهامة للبنية الموجهة نحو الخدمـات SOA التي قد يتعرض لها كل من المختصين في تقنية المعلومات والإدارة المعنية عند مناقشة العمليات الخاصة بالبنية الموجهة نحو الخدمات SOA، وهذه المفاهيم هي:

- **تحبب (تقسيمات) مكونات البنية الموجهة نحو الخدمات (SOA Component Granularity):** وهو يصف لنا حجم المكونات التي تشكل النظام، إذ يحاول أي تطبيق بنية موجهة نحو تقديم خدمة (SOA) أن يشـكل مكونات أكبر أو مكونات محببة خشنة تعرف بخدمات الأعمال. وهي التي يتم بناؤها عادة من مكونات أخرى أصغر تدعى مكونات الحبيبات الناعمـة وكذلـك من خدمات فنية موجودة مسـبقاً. وهذا واقعـي لأن المكونات ذات الحجـم الكبير تجعل عملية فهم وإدارة وإعادة اسـتخدام خدمـات البنية الموجهة نحو تقديم الخدمة (SOA) أكثر سهولة بالنسبة للمؤسسة.

شكل توضيحي (١٣-١)

دور مجمع خدمات البنية الموجهة نحو الخدمات SOA

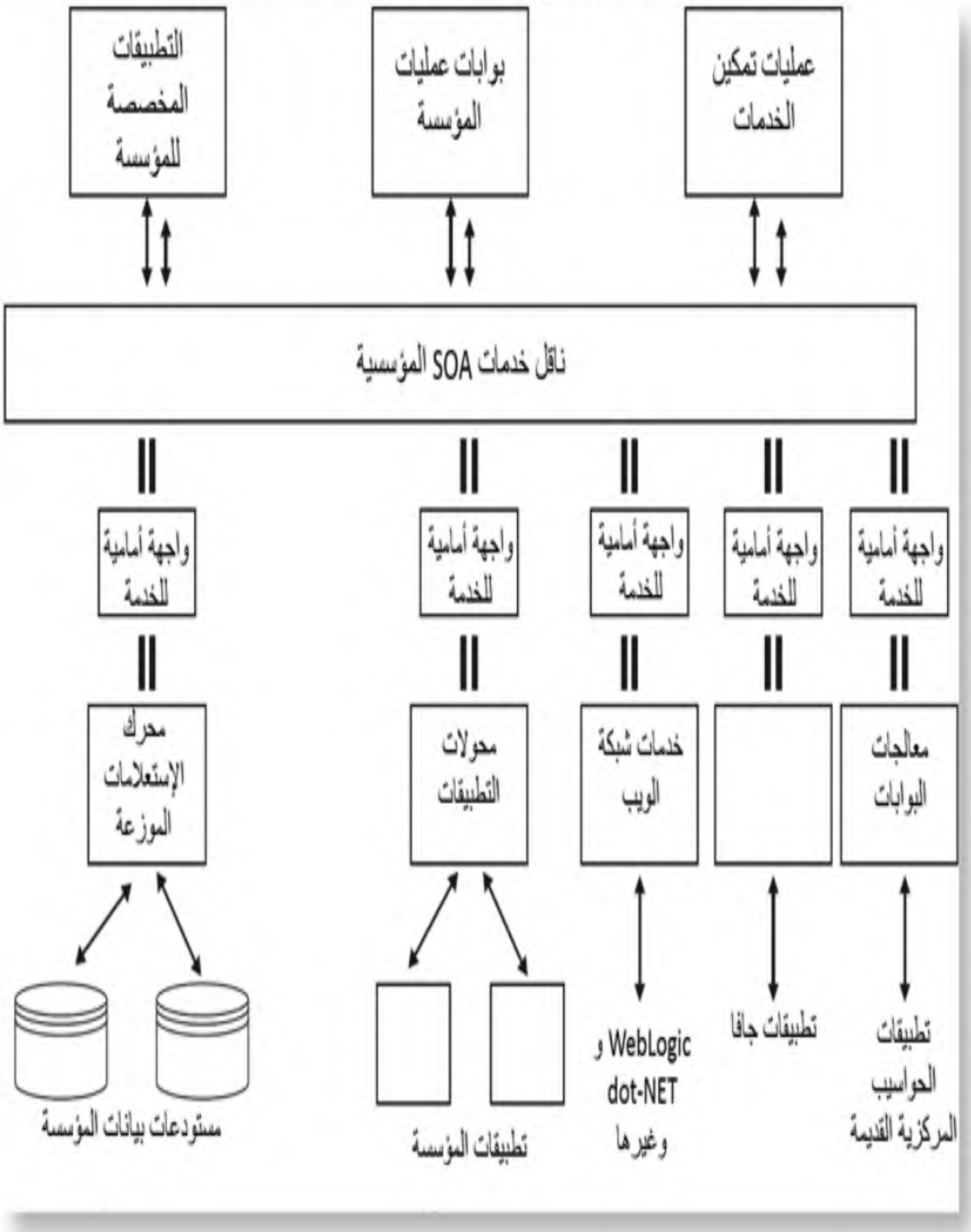


- **واجهـة الخدمة مقابل مفاهيم التطبيـق:** قم بفصل ما تفعله الخدمة عن الكيفية التي تمكنها من فعل ذلك. ويعد ذلك أمراً هاماً نظراً لتبسيطه للمبدأ الذي يشير إلى أنه يجب أن تركز رؤية مسـتخدم الأعـمال للبنية الموجهة نحو الخدمات SOA على ما سـتفعله الخدمة بدلاً من تركيزه على تفاصيل عمل التقنية غير المرئي، قياساً على نظام السيارات.
- **عقـود البنيـة الموجهة نحو الخدمـة SOA:** قم بتحديد الالتزامات بـين مقدم الخدمة والمسـتهلك أو طالـب الخدمة. وقـد يتضمن ذلك احتمالات أو توقعـات للخدمة مثل الإتاحـة والاعتماديـة ومؤشرات الأداء الأساسـية KPIs والتكلفة والدعـم الفني. ويعد ذلك أمراً هاماً نظراً لأنه يسـاعد مسـتخدمي الأعمال على اتخاذ قرارات أعمال منطقية وعقلانيـة فيما يخـص اختيار الخدمات التـي يمكنهم الاعتماد عليهـا. إن هذه المبادئ مشابهة لاتفاقيات مستوى الخدمة المطروحة في الفصل السابع عشر من هذا الكتاب.
- **مفاهيـم التقـارن أو الارتبـاط الضعيـف (Loose Coupling) في البنية الموجهة نحو تقديم خدمة (SOA):** وهي الطريقة التي تسـتخدم لتصميم خدمات أكثر مرونة وأقل اعتماديـة بعضها على بعض. ويسـاعد ذلك في ضم الخدمات وإعـادة تجميعها معاً أو دمجها أو إعادة تركيبها. تعد البيئة الخاصة بالبنية الموجهة نحو الخدمات في ظل وجود عمليـة التقارن او الارتباط الضعيف loose coupling من الأمور الهامة نظراً لأن عملية تجميع حلول الأعمال من الوحدات البرمجية السـابق إنشـاؤها تكون أسرع من عملية كتابة كل وظيفة عمل جديدة من البداية.

إن عملية تبني أو اعتماد المؤسسة للبنية الموجهة نحو الخدمات SOA ليست عبارة عن عملية إجراء تطبيق واحد في المرة الواحدة ، وإنما هي بنية أو هيكلة شاملة يتم من خلالها تنظيـم وربط جميع عمليات تقنية المعلومات بعضها مـع بعض. فالخدمات المقدمة من خلال تطبيقات الإنترنت حيث يمكن للمسـتخدم من أن يقوم بسـحب أي مرجع HTML فقـط من خـلال قيامه بالنقر المزدوج عليه لهو خير مثال عـلى مفهوم البنية الموجهة نحو الخدمات SOA. يوضح الشـكل التوضيحي (١٣-٢) التكوين الافتراضي للبنية الموجهة نحو الخدمات SOA على مستوى المؤسسة.

شكل توضيحي (١٣-٢)

التركيب الخاص بالبنية الموجهة نحو الخدمات على مستوى المؤسسة



يوجد في المستوى السفلي من الشكل مصادر بيانات المؤسسة ونظم أخرى متعددة المنصات. سيتم تعريف جميع العناصر على أنها خدمات كأحد التطبيقات الخاصة على سبيل المثال، والذي ربما تم بناؤه من خليط من مكونات الخادم أو الحاسبات المركزية القديمة أو تطبيقات الويب حيث تم تجميعها مع المكونات المطلوبة من خلال ناقل الخدمة الموائم أو التطبيق المناسب. عندما تحتاج أي من خدمات التطبيقات تلك لعنصر من عناصر البيانات (خدمة أخرى) فإنه سيتم رفع الطلب إلى ناقل الاتصالات ثم يعود إلى مصدر البيانات المناسب. سيتم بناء مثل هذا التطبيق الشامل باستخدام أدوات تطوير برامج التطبيقات المقدمة من قبل المورد (البائع) كمايكروسوفت دوت نت[٢] Microsoft Dot Net أو أوراكل بيا ويب لوجيك[٣] Oracle's BEA WebLogic، وسيتم تهيئته وتنسيقه من خلال عمليات محددة وواضحة.

في الغالب لن يجد المسئول التنفيذي في المؤسسة والمعني بهذا الأمر مثل هذه البيئة الكاملة للبنية الموجهة نحو الخدمات في المؤسسة التقليدية. وإنما ستقوم إدارة تقنية المعلومات المؤسسية وبدعم من إدارتها بتطبيق البيئة الخاصة بالبنية الموجهة نحو الخدمات خطوة خطوة بشكل نموذجي، متبعة في ذلك المخطط الشامل لبناء مثل هذا النموذج. فمع زيادة نمو استخدام خدمات الإنترنت التي أحاطت معظم برمجيات وبيئات تقنية المعلومات المباعة والمقدمة كمكونات برمجية مستقلة بدلاً من أن تكون تطبيقات كاملة، يستطيع كبار مديري الأعمال أن يتوقعوا مشاهدة العديد من تطبيقات البنية الموجهة نحو الخدمات المتقدمة SOA الجزئية أو حتى الكاملة.

حوكمة البنية الموجهة نحو الخدمة وقضايا الرقابة الداخلية والمخاطر:

لا تتم عملية تحول المؤسسة إلى بيئة البنية الموجهة نحو الخدمات الخاصة بتقنية المعلومات فقط من خلال قيامها بشراء حزمة من البرمجيات وبتدريب الكادر التقني على استخدامها ومن ثم افتراض توجه الكادر نحو تطبيقه والعمل به. إن البنية الموجهة نحو الخدمات SOA هي أكثر من مجرد طريقة جديدة لتنظيم نظم تقنية المعلومات الموجودة حالياً، فهي بحاجة إلى تخطيط مفصل للانتقال إلى تلك البيئة الجديدة، وكذلك إلى سياسات وإجراءات جديدة لتقنية المعلومات. وما هو أهم من ذلك، هو حاجتها إلى

تطبيــق تدريجي ومنظم جــداً بحيث يتم جلب عمليات تقنية المعلومــات إلى بيئة البنية الموجهــة نحــو الخدمات SOA بطريقــة مُحْكَمة. في بعض الحالات نــرى أن مزايا وفوائد العمليات التشغيلية للبنية الموجهة نحو الخدمات SOA ستكون واضحة أمام كبار المديرين وغيرهم. على سبيل المثال، فإن أي مؤسسة قامت بتحويل قسم كبير من تطبيقاتها إلى بيئة الويب المعتمدة على جافا Java أو دوت نت Dot-Net، فإنها تســتطيع غالباً وبكل سهولة تبريــر وتأييد مزايا تحول أنظمتها القديمة والعمليات الأخــرى إلى بيئة البنية الموجهة نحو الخدمات SOA.

ينبغي على كبار المديرين المعنيين تكوين فهم جيد وعام عن عمليات البنية الموجهة نحو الخدمــات SOA، هذا بالإضافة إلى فهم بعض الخطوات الضرورية اللازمة لإدارة المؤسســة ولمهــام تقنية المعلومات لديهم لكي يتم الانتقال إلى البنيــة الموجهة نحو الخدمات SOA. بعــض تلك الخطوات تتطلب فهم الضوابط الداخلية لحوكمة تقنية المعلومات، كما تحدثنا في الفصــل الرابع من هذا الكتاب. كما ينبغي أيضاً على كبار المديرين أن يكونوا مرنين مع ضوابط البنية التحتية لتقنية المعلومات الخاصة في بيئة البنية الموجهة نحو الخدمات SOA، هذا بالإضافة إلى فهمهم الجيد لضوابط إدارة المشروعات، كما ســنرى في الفصل الســادس عشر من هذا الكتاب. يحتاج المدير العام المهتم إلى فهم القليل من خصائص البنية الموجهة نحو الخدمات SOA وحوكمتها وقضايا الرقابة الداخلية والمخاطر المتعلقة بها. ســنتحدث في هذا الفصل باختصار عن تطبيق العمليات الفعالة الخاصة بالبنية الموجهة نحو الخدمات SOA، من وجهة نظر حوكمة تقنية المعلومات. وســتناقش الأقســام التالية أهمية كل من إعداد المخططات الأولية والتفصيلية لتطبيق البنية الموجهة نحو الخدمات SOA وتنظيف التطبيقات والعلميات القائمة حالياً بشــكل استباقي، وتأسيس سياسات وإجراءات مناسبة للبنيــة الموجهة نحو الخدمات SOA وفحص وتطبيق البنية الموجهة نحو الخدمات SOA ، بطريقة فعالة.

تخطيط وبناء مخطط تطبيق البنية الموجهة نحو الخدمة وتنفيذه:

يشــير الحرف الثالث للاختصار SOA إلى (البنية) Architecture، فإنشاء البنية الفعالة يعــد بمثابة الخطوة الأولى الأساســية لإطلاق بيئة البنية الموجهة نحــو الخدمات SOA في

المؤسســة. قد يكون المدير التنفيذي للمعلومات CIO في المؤسســة قد تعرض للمفاهيم الخاصة بهذا المصطلح أو أن تكون المؤسسة قد قامت بتنفيذ تطبيق مفرد شبيه ببيئة البنية الموجهــة نحو الخدمات SOA والذي نــال الكثير من التعليقات الحماســية والثناء، ولكن المؤسســة بحاجة إلى بناء خطة شــاملة أو إطار عمل لإطلاق أي تطبيق أو تنفيذ أي عملية تخص البنية الموجهة نحو الخدمات SOA.

إن الفكرة الرئيسية للوصول إلى البنية الفعالة الموجهة نحو الخدمات هو تحديد الخطة الموجــودة أو بناء الخدمة باســتخدام الوحدات المبنية التي ســتعرف SOA. وكما تحدثنا ســابقاً، فإنه يجب أن تظهر خدمات SOA كما لو كانت أشبه بمجموعة من القطع الخاصة بلعبة الليغو LEGO، وهي لعبة الأطفال الشائعة حيث يمكن من خلالها تركيب تلك القطع لتكوين مجموعة مختلفة من الهياكل المعقدة ثم يتم فصل بعضها عن بعض لتركيب هيكل أو شكل آخر مختلف. على كل حال، فإن خدمات SOA أكثر من مجرد قطع خاصة بلعبة الليغــو والتي يمكنها فقط أن تكون بأشــكال مكعبات أو مثلثات. فخدمات SOA أوســع بكثــير وقد يكون لها العديد من الأبعاد المختلفة عمومــاً. لذا ينبغي أن تحدد بنية SOA للمؤسســة عناصر الخدمات المختلفة الخاصة بها والمستفيدين من الخدمات، هذا بالإضافة إلى مســار تدفق النشاطات ونقاط اتخاذ القرارات بين المســتفيدين المعنيين بالعملية على النحو التالي:

- **أصحاب الأعمال:** يعمل المالك أو مســتخدم النظم على توفير متطلبات التطبيق اللازمة لتنفيــذ أحد القدرات أو الحلول أو العمليات الجديدة الخاصة بالأعمال. كما يجب على صاحــب العمل أو أعضاء فريق دعم تقنية المعلومــات أن يقوموا بتطوير نماذج الأعمال business models وذلــك لتســهيل فهــم أي متطلبات خاصة بخدمــات تطبيق تقنية المعلومــات. كما يحتاج صاحب العمل أيضــاً إلى تحديد المتطلبات غير الوظيفية كجودة الخدمة المتوقعة بالنسبة للقدرة أو الحل أو العملية.
- **مهندســو SOA:** لإطلاق مبادرة البنية الموجهة نحو الخدمات SOA، تحتاج المؤسسة إلى تعيين مهندس ماهر في SOA لكي يقوم بتحليل متطلبات الأعمال والخروج منها بتصاميم خدمات وأعمال. وقد يقرر مهندس SOA على ســبيل المثال، أن يعيد استخدام مكونات

موجودة حالياً بدلاً من إنشـاء مكونات جديدة. وعندما يقترح المهندس تنفيذ خدمة أو عملية جديدة أو التغيير في خدمة أو عملية موجودة، فإنه يجب عليه تسليم مواصفات التصميم الخاصة بمخططات الحالة والنماذج العملية وتصميم الواجهات. كما يعمل مهندس SOA على صياغة المتطلبات غير الوظيفية للمكون المراد تطبيقه بشكل رسمي متضمناً المتطلبات الخاصة بالإتاحة والأمن والأداء الخاصة به.

- **مطورو التطبيقات:** يقوم مطور التطبيقات بتنفيذ المكونات بناءً على مواصفات التصميم المقدمة من مهندس SOA، ووضع الضوابط الداخلية، ووضع خطط الفحص أو الاختبار بناء على هذه المواصفات. وللمساعدة في تحقيق التقارب بين التقنية والمنهجية، فإنه ينبغي على مطور التطبيقات استخدام الأجزاء التي وضعها مهندس SOA من أجل التنفيذ متضمنةً الأكواد البرمجية ونموذج التحسينات.
- **مدير الجودة:** يجب على مدير الجودة في المؤسسة أن يستخدم المدخلات التي قام كل من صاحب العمل والمهندس والمطور بتقديمها لمراجعة وتدقيق مدى صحة الخدمة أو العملية التي تم تنفيذها. ثم يقوم مدير الجودة بعد ذلك باستخدام خطط الفحص أو الاختبار التي قام المطور بتسليمها ليقوم بتنفيذ اختبار الحلول المقدمة في البيئة التجريبية ويتحقق من سلامة مقاييس الجودة والآثار الجانبية والخصائص غير الوظيفية.

بمجرد أن يتم تحديد الفريق الرئيسي للعمل، فإنه ينبغي على المؤسسة تطوير مخطط لبيئة SOA الذي يشير إلى حالة الهدف المطلوب، أو إلى الصورة الكاملة لما ينبغي أن يظهر به تطبيق SOA بعد اكتماله. يجب على مخطط SOA في المقام الأول أن يضع كل خدمات الأعمال التي يتعين القيام بها ومتطلبات وصف الخدمات ذات العلاقة ومقاييس الأداء ومعايير التشغيل البيني أو التبادلي.

إن من شأن مخطط كهذا أن يقدم ملخصاً شاملاً وحتى "أوامر السير" بشأن الوضع الذي ترغب المؤسسة وإدارة تقنية المعلومات في الانتقال إليه مع SOA. بالطبع فإنه يجب على المؤسسة ألا تبدأ بتنفيذ أو حتى توافق على إستراتيجية SOA ما لم يكن هناك فهم جيد للفوائد التي سيتم تحقيقها من هذا النهج. يوضح الشكل التوضيحي (١٣-٣) بعض الفوائد الرئيسية التي يجب أن تدركها المؤسسة جراء الانتقال إلى بيئة SOA.

انتقال التطبيقات والعمليات القائمة حالياً إلى بيئة SOA:

إن انتقــال العمليات والتطبيقات الموجودة ســواء كانت نظماً قديمة أو تطبيقات قائمة على الخادم أو تطبيقات أكثر حداثة كتطبيقات الهواتف المحمولة القائمة على شبكة الويب قد يشــوبه بعض التحديات نفســها والتي قــد يتذكرها بعض العاملــين القدامى في أواخر تســعينيات القرن الماضي وهو الخوف من مشــكلة العام ٢٠٠٠ (Y2K). وعلى الرغم من نسيان معظم الأخصائيين لذلك، فإن العديد من البرامج القائمة على لغة البرمجة COBOL التــي تم بناؤها في تســعينيات وثمانينيــات القرن الماضي أو حتى قبــل ذلك الوقت، كانت بهــا حقول خاصة بـتاريخ التقويــم النظامي بالصيغة yymmdd. وقــد اعتمدت العديد مــن القرارات البرمجية المرتبطة بتواريخ مختلفة على اتخاذ الإجراءات النظامية عن طريق ترتيب هذه التواريخ. وقد تســبب العام ٢٠٠٠ في تســجيل هذه القرارات البرمجية القائمة على التاريخ بـ ٠٠٠٠. لقد كانت المخاوف تدور حول أن العديد من النظم ســوف تتوقف نظراً لتواريخ البرامج غير الصالحة والخارجة عن المدى أو التسلســل، كما أن عملية التوثيق بالنسبة للعديد من التطبيقات وقتها كانت ضعيفة. وقد بذلت الإدارات الرئيسية ومدققو تقنية المعلومات جهوداً كبيرة للاستعداد لمشكلة Y2K.

شكل توضيحي (١٣-٣)

الفوائد الرئيسية جراء استخدام بيئة SOA

فيــما يلي النقاط التي يجب أخذها في الاعتبار مــن قبل إدارة تقنية المعلومات والإدارة العامة في تحول نظم وخدمات تقنية المعلومات الخاصة بهم إلى بيئة البنية الموجهة نحو الخدمات SOA.

تحســين رؤية الأعمال: تعمل بيئة SOA عموماً على تكامل النظم الموجودة وتجميع بيانات من وجهات نظر أكثر ثباتاً ودقةً لبيانات العملاء والتي تتضمن:

- معلومات حتى هذه اللحظة لتحسين خدمة العملاء.
- معلومات عبر المؤسسة تستهدف (١:١) من النشاطات.
- معلومات متناغمة ودقيقة وأكثر شمولاً تساعد على اتخاذ قراراتٍ أفضل.

تحقيــق مرونة الأعمال: في حــال التطبيق الكامل، بإمكان بيئة SOA إيجــاد بنية تحتية لبرامج تكاملية ورشيقة لتحقيق الاستجابة السريعة لحاجات الأعمال:

- التسليم السريع لقدرات الأعمال الجيدة.
- يقلل الآثار الناجمة عن تغير الأعمال والتقنية.
- حماية الاستثمارات أثناء خلق وظيفة جديدة.

كسب كفاءة الأعمال: تبسيط وأتمتة وتمكين تتبع ورؤية أفضل لعمليات الأعمال في المؤسسة:

- مشاركة وتبادل عمليات الأعمال بشكل سري داخل وخارج الجدار الناري لنظم تقنية المعلومات.
- إنشاء جسور بين مخازن البيانات لضمان سلامة البيانات على نحو أفضل.
- إدارة القــرارات الخاصة بالأعمال بصورة اســتباقية من خلال مؤشرات أداء رئيســية من مصادر أخرى.

تحسين عمليات حوكمة تقنية المعلومات: نظراً لقيام بيئة SOA بتصنيف وتنظيم جميع عمليات تقنية المعلومات في المؤسســة بشكل أفضل، فإنه ســيتم إدارة وضبط الحوكمة والرقابة الشاملة لهذه العمليات بشكل أفضل.

وتتعرض إدارات تقنية المعلومات لبعض القضايا المشـابهة عندما تخطط وتعد للتحول إلى SOA. وفي حـين أن المخـاوف هذه الأيام ليسـت في تواريـخ COBOL ذات الصيغة yymmdd غير الموثقة، فإن الإدارة التقليدية لتقنية المعلومات لديها طبقات من التطبيقات والبرامج والنظم الزائدة التي لا يمكن الوصول إليها في الغالب على نحو متبادل (ومشاركتها)، وكذلـك العديد من التكاملات غير المتناغمة التي تحدث من نقطة إلى أخرى في تطبيقاتها. وربما تمثل هذه المشـاكل التحدي الأكبر في موضـوع تطبيق العمليات الفعالة لبيئة SOA. وبالنسبة لأي فريق يقوم بتطبيق بيئة SOA على مستوى المؤسسة، إذا لم يكن هذا الفريق مُلماً بالنظم والعمليـات والهياكل التنظيمية لتقنية المعلومات القائمة حالياً فهناك احتمال قوي أن يفشل تطبيق SOA.

سياسات وإجراءات بيئة SOA:

إن المفهوم العام الشـامل والرائع لبيئة SOA هو أنها تقوم باسـتخدام وحدات خدمية يمكـن تجميعها وإعادة تجميعها أسـوة بالمثال الذي أشرنا إليه سـابقاً عن القطع الخاصة بـلعبة الليغو. على كل حال، فإن بيئة SOA لن تعمل في المؤسسـة على نحو جيد في حال قـررت إحدى وحدات الأعمال فيها بأنها تريد أن تكون مختلفة بعض الشيء وأن الوحدات الخدمية الخاصة بها في الواقع لا تتناسـب مع غيرها. فباستخدام مثالنا الخاص بقطع لعبة الليغو، فربما يكون هناك وحدة معينة ترغب في أن تكون القطع الخاص بها بحجم مختلف، وهي في هذه الحالة لن تتناسب مع أي من الوحدات الأخرى.

وعلى الرغم من أن هناك دائماً أسـباباً وراء حاجة وحدة أو أخرى من وحدات الأعمال إلى أن تكون مختلفة (كالقضايا الأمنية العالية)، فمن الطبيعي أن تحتاج المؤسسـة إلى نوع من أنواع السـلطة المنوط بها وضع المعايير، وذلك لوضع السياسات وسن القوانين المتعلقة بخدمات SOA الخاصة بها. بالنسـبة للعديد من المؤسسات، فإن الكيانات الحكومية التي تقوم بوضع وفرض السياسـات الخاصة بـ SOA ومعايير المؤسسة تسمى عادة مراكز SOA للإبـداع أو مراكز الجـدارة SOA. وتتكون مراكز الجدارة تلك من ممثلين أو وكلاء من كل وحدة من وحدات الأعمال التي تتأثر بمخطط وخطط SOA الخاصة بالمؤسسة. فتقريباً كل جزء من أجزاء مخطط SOA الخاص بالمؤسسة - متضمناً ذلك الخدمات التي سيتم بناؤها،

وكيفية تحديدها، وكيفية التشغيل البيني لها - سيقوم بتعريف سياسات SOA الخاصة بالمؤسسة بشكل ضمني. ونظراً لاحتواء مخطط SOA الخاص بالمؤسسة على العديد من السياسات الضمنية، فمن المهم جداً أن يكون أول إجراء يتخذه مركز الجدارة الخاص بـ SOA والذي تم إنشاؤه مؤخراً، هو التصديق على هذا المخطط واعتباره هدفاً مشتركاً.

ومن المهم بالطبع بالنسبة لكل مجموعة معنية بداخل المؤسسة أن تفهم الآثار الناتجة عن مخطط البنية الموجهة نحو الخدمات (SOA) وتوافق عليها نظراً لتأثيرها في أعمالها ونشاطاتها اليومية. ولهذا السبب، فإن التصديق على مخطط SOA لا يجب أن يأخذ شكل الموافقة الروتينية دون دراسة. بل يجب على كل شخص معني التفكير ملياً ليعرف كيف ستؤثر هذه الرؤية للبنية الموجهة نحو الخدمات SOA فيهم، متضمناً ذلك النتائج الشاملة لحوكمة تقنية المعلومات.

ينبغي على المؤسسة وضع سياسات الامتثال لمتابعة وتقييم التنفيذ الإلزامي لسياسات وعمليات بيئة SOA الخاصة بها. هذا من شأنه أن يضع "قواعد الطريق" ويوفر الحكم على نشاطات بيئة SOA القائمة على المخطط المتفق عليه. إن عمليات التنفيذ الآلي مفضلة عن التنفيذ حسب المكان الذي يمكن أن تطبق فيه. على كل حال، لا يمكن أتمتة جميع السياسات، فقد يكون هناك بعض الخطوات التي تتطلب التقييم والتدخل البشري.

تغطي الحوكمة السليمة لبيئة SOA عدة نقاط إلزامية خلال الدورة الكاملة لحياة الخدمة. يصف الشكل التوضيحي (١٣-٤) أدوار ومسؤوليات الأشخاص الرئيسيين المشاركين في تطبيق بيئة SOA والذين أصبحوا جزءاً لا يتجزأ من دورة حياة تطوير النظم الخاصة بتلك البيئة. سيتم الحديث عن المفاهيم الخاصة بدورة حياة تطوير النظم System Development Life Cycle (SDLC) وأهميتها في حوكمة تقنية المعلومات في الفصل الخامس عشر من هذا الكتاب والذي يدور حول موضوع تطبيق نظم تقنية المعلومات المتكاملة. يتم تقسيم سياسات وعمليات بيئة SOA عادة إلى فئتين هما: (١) سياسات حوكمة أثناء التصميم لضمان توافق أدوات بيئة SOA مع متطلبات التصميم المنصوص عليها في مخطط بيئة SOA. (٢) سياسات حوكمة أثناء التنفيذ لضمان توافق خدمات SOA مع متطلبات التشغيل التي تم التفاوض بشأنها

بـين مقدم الخدمة والمسـتهلك. إن هذه العمليات الخاصة بحوكمة بيئة SOA تشـبه بعض الشيء اتفاقيات مستوى الخدمة SLAs التي تمت مناقشتها في الفصل السابع عشر من هذا الكتاب، حيث سـتقبل العمليات التشـغيلية لتقنية المعلومات بشـكل رسمي بتوفير التعاملات الخاصة بمجموعة المسـتخدمين وفقاً لجدول زمني متفق عليه مسبقاً، كما سـتقوم تقنية المعلومات بتسليم ملف التحديثات والعمليات المنجزة وفقاً للجدول الزمني نفسه المتفق عليه. فمن خلال SOA يمكن أن نقوم بعمل سلسلة من الاتفاقيات الصغيرة بين مقدمي ومستهلكي الخدمات.

شكل توضيحي (١٣-٤)

أدوار ومسؤوليات أصحاب المصلحة خلال دورة حياة بيئة SOA.

تقوم دورة حياة بيئة SOA بوصف وتنفيذ سلسـلة من النشـاطات ونقاط اتخاذ القرار بين أصحاب المصلحة – مستخدمين وتقنية معلومات – المعنيين بهذه العملية. ينبغي أن تشتمل دورة حياة تطوير بيئة SOA الفئات التالية من المشاركين الرئيسيين:
أصحـاب الأعـمال: يقوم أصحـاب الأعمال في بيئة SOA بتوفـير المتطلبات اللازمـة للأعمال المزمع تنفيذهـا متضمناً ذلك الإمكانـات أو الحلول أو العمليات. وأفضل طريقـة لصياغة هذه المتطلبات هو أن يتم وضعها في نموذج عمليات الدعم والذي يقوم بتغطية نشـاط الخدمة. فاسـتخدام نماذج العمليات يسـهم في توفير بيئة تجعل عملية فهم متطلبات تطبيق تقنية المعلومات أكثر سهولة. كما يحتاج صاحب العمل أيضاً إلى تحديد الاحتياجات غير الوظيفية (مثل جودة الخدمة) للقدرة أو الحل أو العملية.
المهندس المعماري لبيئة SOA: عادة ما يقوم المهندس المعماري لبيئة SOA، بصفته عضواً أساسياً في فريق تقنية المعلومات، بتحليل متطلبات الأعمال وتقسيمها إلى عناصر خاصة بتصميم عملية الخدمة. فقـد يقرر المهندس إعادة اسـتخدام أحد المكونات الموجودة بدلاً من إنشـاء مكون جديد. في هذه الحالة فإنه سيقرر تحويل هذا المكون إلى عنصر في دورة حياة بيئة SOA ليتمكن من إعادة استخدام هـذا المكـون القائم حاليـاً. عندما يتم تحديد الخدمـة أو العملية الجديدة أو المـراد تطبيقها، فإن مهندس SOA يقوم بتسـليم مواصفات التصميم في شكل مخططات الحالة ونماذج العملية وتصاميم للواجهـات الأماميـة. كما يعمل مهنـدس SOA على صياغة المتطلبات غـير الوظيفية للمكون المراد تطبيقه بشكل رسمي متضمناً الإتاحة والأمن والأداء.

مطــور بيئة SOA: يقوم المطور بتنفيذ المكونات بناءً عــلى مواصفات التصميم المقدمة من مهندس بيئــة SOA كما يقوم أيضاً بإنشــاء خطط اختبار بناءً على هذه المواصفات. وللمســاعدة في تحقيق التقــارب بين التقنية والمنهجية، فإنه ينبغي على المطور اســتخدام الأجزاء التي وضعها مهندس SOA لتطبيقها متضمناً ذلك الأكواد البرمجية وأدوات تحسين النموذج.
مديــر الجــودة في بيئة SOA: يســتخدم مدير الجــودة المدخلات التي قام كل مــن صاحب العمل والمهنــدس والمطــور بتوفيرها لمراجعة وتدقيق مدى صحة الخدمة أو العمليــة التي تم تنفيذها. ثم يقوم مدير الجودة بعد ذلك باســتخدام خطط الفحص أو الاختبار التي قام المطور بتســليمها ليقوم بتنفيذ اختبار الحلول المقدمة في البيئة التجريبية والتحقق من سلامة مقاييس الجودة والآثار الجانبية والخصائص غير الوظيفية.
مشــغل بيئة SOA: يقوم المشــغل باســتقبال الحلول التي تم اختبارها والتأكد مــن صحتها ويقوم بتطبيقها داخل العمليات المعيارية لتقنية المعلومات لجعل هذا الحل متاحاً للمستخدمين والمستهلكين له. حيث يقوم هو أو هي باستخدام المواصفات التي تمت صياغتها والخاصة بالمتطلبات غير الوظيفية لتشغيل الحلول الافتراضية التي تتفق مع اتفاقيات مستوى الخدمة SLAs المطلوبة من قبل مستهلكي التطبيقات. إن الحلول الخاصة بحوكمة تشــغيل SOA هي التي تقدم هذه الأنواع من القدرات من خلال فرض المتطلبات غير الوظيفية واتفاقيات مستوى الخدمة.

سياسات بيئة البنية الموجهة نحو الخدمات SOA خلال فترة التصميم:

إن العنــصر الرئيسي في سياســات وعمليــات بيئة SOA وقت التصميــم هو ضمان أن الخدمات ســيتم بناؤها وفقاً للمواصفات المحــددة في الخطة الخاصة بمخطط بيئة SOA. وعلى وجه الخصوص، فإنه ينبغي تصميم سياسات لضبط وتقييد تصرفات وسلوك مصممي ومطوري الخدمات نيابة عن كل جهود بناء بيئة SOA في المجالات العامة التالية:

- **قابلية التشــغيل البيني:** لا بد من التصريح في مخطط SOA عن وســائل موحدة لتوفير التشغيل البيني بين خدمات تقنية المعلومات. ويكون ذلك عادة من خلال مجموعة من المعايير.
- **قابلية الاكتشاف:** قد تحتاج الخدمات لسمات أو خصائص محددة كوصف سهل للعمل ومعلومات متعلقة بموقع الخدمة داخل بيان للتصنيف أو التســجيل الذي قد تم إنشاؤه

مــن قبل. إن هذه العناصر تجعل من الممكن اكتشــاف ومعرفة الخدمات التي يمكن أن تُحدد أو تُعرف لاحقاً من خلال السياسة.

- **الأمن:** ينبغي التصريح في مخطط SOA عن وسائل موحدة لتوفير الأمن عبر جميع خدمات SOA. كما ينبغي أن يكون نمط ومعاملات هذا الأمن متســقاً مع كل الممارســات الخاصة بحوكمة أمن تقنية المعلومات في المؤسسة. كما ناقشنا في الفصل العاشر من هذا الكتاب.
- **التفرد:** لا يجب أن يكون للخدمات الجديدة أســماء الخدمات نفســها التي تم إنشاؤها من قبل. يمكن للسياسات أن تساعد في التأكد من أن المجموعات لا تواجه هذه المشكلة.
- **امتثال الواجهة:** إن طريقة اســتخدام وتدشــين جميع الخدمات يجب أن تكون موحدة. ومــع أن خدمات SOA تعد أكثر من مجرد عناصر برمجيــة لتقنية المعلومات، فإن هذه العملية مشابهة لأمر التشغيل Run Command الموجود في نظام ميكروسوفت ويندوز. لذا يجب أن يتم فرض هذا الشكل المعياري للواجهة عن طريق السياسة.
- **امتثــال صيغ البيانــات:** كما ذكرنا، يجب أن يكون الهــدف الرئيسي لخدمات SOA هو إعادة اســتخدام عناصر الخدمات. فالطريقة الشــائعة للمحافظة على هذه الميزة (إعادة الاستخدام) هي إنشاء صيغ بيانات مشتركة تُعرف بالمخططات schemas. إذ القيام بهذا العمل ســيضمن إمكانية اســتخدام حقل العنوان التابع لإحدى الخدمات من قِبل خدمة أخرى حتى لو كان هناك اختلاف في الطريقة التي تُخَزِن بها الخدمات بياناتها. لذا يجب أن يتم فرض المخططات المشتركة عن طريق السياسة.
- **المقاييــس:** يجب أيضاً القيام بوضع معلومات وتقاريــر إحصائية تتعلق بقضايا تصميم الخدمة من خلال السياســة. لن تتمكن المؤسســة ولا فريق تدقيق تقنية المعلومات من قياس العمليات التشغيلية لبيئة SOA ما لم يكن هناك بعض المقاييس الموضوعة لكل من الأهداف والحد الأدنى من معايير الأداء الخاصة بالتشغيل.

يجــب أن تتصــل عمليات SOA خــلال التصميم بصورة نمطية مــع دورة حياة تطوير النظم SDLC الخاصة بالمؤسســة. وسيتم الحديث عن دورة حياة تطوير النظم وأهميتها في حوكمــة تقنيــة المعلومات في الفصل الخامس عشر من هــذا الكتاب. كما يمكن تطوير

دورة حياة تطوير خدمات مشــابهة في هذه الحالة. إن اعتماد بيئة SOA يطرح تحديات بالنســبة للمؤسســات التي اعتادت اســتخدام تطبيقات تقنية المعلومات كوسيلة لمعالجة المتطلبات الخاصة بالتطبيقات. عادة ما يشار إلى الهياكل والعمليات الجديدة بدورة حياة SOA والتي تكون مطلوبة لتوفير الأســاس للرشــاقة التنظيمية وتروج لنجاح عملية اعتماد بيئة SOA. حيث أصبح دمج عمليات دورة حياة SOA مع الهياكل التنظيمية الفعالة من العناصر الرئيسية في إطلاق العمليات الفعالة لبيئة SOA.

تقع معظم أقســام تقنية المعلومات في المؤسســة تحت ضغط شــديد من أجل تقديم حلــول فعالة من حيث التكلفة والوقت لعمليات التشــغيل الخاصــة بأعمالها. ولتحقيق أهــداف هذه الحلول فإن هــذه الإدارات تســتخدم مكونات ووحدات تقنيــة وتنظيمية مشتركة، هذا بالإضافة إلى استخدام المبادرات التي تتم عبر المشاريع، وذلك لتعزيز التعاون من خلال قســم تقنية المعلومــات. فعندما يتم الجمع بين هذه الحلــول العقلية الخاصة بتقديــم الخدمات (كما هو الحال في الخدمــة ذات القيمة وليس كما في التقنية)، فإنه من الممكن لإدارة تقنية المعلومات أن تجد نفسها تتحرك باتجاه الطريق المؤدي إلى بيئة SOA.

وكجــزء من هذا الطريق المؤدي إلى بيئة SOA، فإنه ينبغي على جميع الأطراف ســواء كانــت تقنية المعلومــات أو الإدارة أن يكون لديهم العقلية التي تفكر من حيث سلاســل القيمــة والتي تدرك أن هذه الخدمــة هي عبارة عن شيء تم إيجاده لتحقيق رضا العملاء. ومع أنه لا يمكن إنكار أن القول أســهل من التطبيق الفعال، فإن المؤسســة بحاجة إلى إنهاء التفكــير التقليدي بالتطبيقات المركزية، وذلك من خــلال تطبيق عمليات تنظيمية مهيكلة تتخطــى حدود المــشروع ودورات حياتها. عندمــا تتحد العقلانية والمنهجية والأشــخاص والمنظمــة والتقنية بشــكل ناجح، عندهــا يمكن أن يعود تبنــي SOA بفوائد عظيمة على المؤسسة من حيث الحجم والفاعلية وخصوصاً الخفة والرشاقة.

سياسات وعمليات بيئة SOA خلال التشغيل:

يتضمن وقت التشغيل عملية التطوير بالكامل، والتجريب، والإنتاجية لنظم بيئة SOA. وسينتج عن سياسات الحوكمة خلال التشغيل احتكاكات سياسية أقل داخل المؤسسة نظراً

لأنها في الغالب تقيد نظم تقنية المعلومات بالنيابة عن مستهلكي خدمة SOA. بالنسبة للجزء الأكبر، فإن السياسات الخاصة بوقت التشغيل تكون موجودة للتأكد من أن الخدمات تعمل "كما ينبغي" طبقاً لتوقعات متلقي الخدمة. ويشمل هذا:

- **اتفاقيات مستوى الخدمة SLAs:** تمت مناقشة هذه الاتفاقيات في الفصل السابع عشر من هذا الكتاب. حيث يجب أن يتفق كل من مقدمي خدمات SOA ومستهلكيها على التوقعات الخاصة بالأداء طبقاً لاتفاقية مستوى الخدمة، هذا بالإضافة إلى المقاييس التي تثبت بأن الخدمات تعمل كما هو متوقع.
- **التحقق:** يجب أيضاً أن يتفق كل من مقدمي ومستهلكي الخدمات على الطريقة التي يجب اتباعها لتحديد هوية المستهلكين للتعريف عن أنفسهم. فبناء على معايير الحوكمة الخاصة بوقت التشغيل، فإنه ينبغي أن يتضمن التحقق قضايا مثل نظم تحديد الهوية واستخدام بطاقات الأمن.
- **التصريح:** يجب أن يكون هناك عمليات أمنية معمول بها لتحديد ما إذا كان مقدم الخدمة مسموحاً له استدعاء الخدمة أم لا.
- **التشفير:** وهو جزء من العمليات القوية لأمن المعلومات. لذا يجب أن يكون هناك معايير تشفير لإبقاء الرسائل مشفرة أو مشوشة بحيث لا يمكن قراءتها بسهولة من قبل أشخاص غير مصرح لهم.
- **التنبيهات والإشعارات:** يجب وضع شروط لإطلاق التنبيهات من خلال إجراءات وذلك لإرسالها إلى المعنيين. ويمكن أن تشير التنبيهات إلى شروط خاصة بالأعمال وكذلك شروط تقنية.
- **المقاييس:** ينبغي وضع مؤشرات أداء رئيسية ومقاييس أثناء التشغيل لتوفير مؤشرات يمكن استخدامها لاحقاً لتقييم الأداء.

تقوم السياسات الخاصة بوقت التشغيل عادة بالتشديد على الفريق المسئول عن عمليات تشغيل تقنية المعلومات ونظم تقنية المعلومات بالنيابة عن مستهلك الخدمة. حيث يمكن أن تشمل هذه العمليات طلبات الدعم الفني والاستجابة الفورية للتنبيهات

والإشعارات. ويعد تمكين طلب الاستجابة الأكثر سرعة لتغيير الشروط الخاصة بوقت التشغيل من الأمور المهمة في بيئة SOA.

تماماً كما هو الحال بالنسبة لنقاط التفتيش الجمركية الموجودة على حدود الدولة والتي تقوم بفحص كل من جواز السفر والأمتعة، فإن العملية الفعالة لحوكمة تقنية المعلومات تضع نقاط تفتيش للتأكد من أن الاتفاقيات بين الإدارات يجري تنفيذها والالتزام بها، متضمناً ذلك مستودع سجل خدمات SOA الذي يعتبر بمثابة نقطة إنفاذ لسياسات وعمليات SOA خلال وقت التصميم. لذا يجب أن يكون لدى نظام برمجيات التحكم وسائل للعمل في نقاط إنفاذ للسياسات والعمليات الخاصة بتشغيل SOA؛ متضمناً ذلك عمليات التحقق من الرسائل، وذلك لضمان التأكد من أنه مصرح لها باستدعاء الخدمة، ويعد هذا أحد المطالب التشغيلية المهمة.

لقد أكدنا أهمية اتفاقيات مستوى الخدمة SLAs في العديد من الأماكن خلال حديثنا عن عمليات بيئة SOA. حيث تقوم اتفاقيات مستوى الخدمة المعرفة جيداً والتي يتم متابعتها على نحو جيد بمراقبة صحة وأداء الخدمة وضمان تقديم الخدمات للمستهلكين كما تم الاتفاق عليه.

تتغير متطلبات وسمات بيئة SOA المشار إليها في الفقرات السابقة باستمرار أكثر بكثير من أي منطق وظيفي للخدمة. لذا يجب أن يدرك كبار المديرين أن المهمة الأساسية لحوكمة بيئة SOA هي تعزيز وضمان السلوك المرغوب فيه بين الأشخاص المشاركين والنظم. كما يجب على إدارة تقنية المعلومات الإفصاح بوضوح عن سياسات بيئة SOA الخاصة بها، ثم تقوم بعد ذلك بفرض هذه السياسات بشكل متناغم وثابت طوال دورة حياة بيئة SOA.

في الأيام الأولى لظهور SOA، كان مهندسو هذه البيئة يقضون عدة أسابيع أو حتى شهور ليقوموا بعملية التوثيق الدقيق لهذه السياسات في كتب ضخمة والتي لم يهتم أحد بقراءتها. وهذا أشبه بالخطط القديمة للتعافي من كوارث تقنية المعلومات التي أصبحت تسمى الآن خطط استمرارية تقنية المعلومات كما وضحنا في الفصل العاشر من هذا الكتاب. فإن لم تكن عملية تحفيز المشاركين على الإلمام بهذه السياسات مسألة تتسم بالصعوبة الشديدة فإن إجراء التغييرات على هذه السياسات سيكون أكثر صعوبة. فقد كانت العمليات القديمة

للمراجعة والموافقة اليدوية لازمة التطبيق لإجبار الجميع على قراءة القوانين الجديدة والالتزام بها. لكن سرعان ما أصبحت هذه المراجعات مأزقاً مما شجع الناس على الالتفاف حول هذه السياسات مما أدى إلى إبطال المهمة الرئيسية لحوكمة SOA.

في حين أن هذا الأمر ينطبق على جميع السياسات الخاصة بتقنية المعلومات، إلا أن الممارسات القوية والفعالة لإدارة سياسة SOA تعد هنا وبشكل خاص من الأمور المهمة. وعلى الرغم من المسؤوليات الحقيقية الملقاة على عاتق إدارة تقنية المعلومات، فإنه يجب التعبير عن سياسات SOA الخاصة بالمؤسسة بصيغ واضحة يمكن تعريفها وتغييرها وإزالتها بسهولة حسب الحاجة. هذا بالإضافة إلى أنه يجب أن تكون العمليات مفعلة لتقوم بإنفاذ تلك السياسات الخاصة ببيئة SOA بصورة فعالة كما هو مطبق طوال دورة حياة SOA. لذا يجب أن يتلقى المشاركون تغذية راجعة فورية من خلال إدارة السياسات التي تعتبر من العناصر الحاسمة في عمليات حوكمة SOA.

تعمل الإدارة الفعالة لسياسات SOA على إزالة العقبات والاعتراضات على حوكمة SOA، وذلك من خلال توفير دليل واضح يتعلق بما هو متوقع أن يكون متوافقاً مع المخطط الموضوع والمتفق عليه لبيئة SOA. لذا نجد أن حلول إدارة السياسات تسهم في تحسين المساءلة وضمان نتائج متناغمة.

البنية الموجهة نحو الخدمة وحوكمة تقنية المعلومات:

لقد تحدثنا عن العديد من جوانب حوكمة تقنية المعلومات المتعلقة ببيئة SOA، ولكن للأسف لم نتحدث إلا عن القليل من السمات والميزات العديدة لبيئة SOA. ففي ظل مفهوم SOA الساعي إلى فصل عناصر الوظائف البرمجية إلى مكونات مستقلة يمكن تبادلها كما يمكن ربطها أو إعادة تعريفها بسهولة، فإننا سنرى وظائف أكثر وأكثر مرتبطة بمفهوم SOA في عالمنا المتقدم المعتمد على شبكة الإنترنت. على سبيل المثال، معظم بائعي برمجيات قواعد البيانات هذه الأيام كشركة أوراكل Oracle، قاموا بتطبيق مبادئ SOA في هياكل قواعد بيانات الخاصة بتخطيط موارد المؤسسة الصادرة عنهم، كما أننا سنرى مزيداً من التركيز على SOA في منتجاتها خلال السنوات القادمة.

نكاد نجزم بأن المؤسسة التقليدية التي تستخدم مجموعة كاملة من أدوات SOA هذه الأيـام لن تبدأ في البداية العمل وفقـاً للنموذج الكامل لتطبيق SOA. وإنما قامت العديد مـن الشركات حتى اليوم بتحويل واحد أو أكثر من تطبيقاتها الرئيسـية إلى نموذج خدمات الويـب، وهو نهج مشـابه لمفهوم SOA. وقـد تم توضيح تلك العمليـة الخاصة بتطبيق خدمات الويـب والخاصة بتحويل أحد التطبيقات الحاليـة إلى بيئة قائمة أو معتمدة على شـبكة الإنترنت في الشـكل التوضيحي (١٣-٥). كما يمكن العثور على مثال من هذا النوع مـن التطبيقات في واحد من الحلول البرمجية الخاصة بـإدارة علاقات العملاء والمقدم من خلال شركة سـيلز فورس.كـوم (www.salesforce.com/company) SalesForce.com، وهي مقدم برمجيات ناجح جداً لا يبيع منتجاته البرمجية من خلال الأقراص المدمجة التي تحتـوي على البرمجيات المطلوبة والمجلدات التـي تحتوى على الوثائق، وإنما كل ما تقدمه شركة سيلز فورس.كوم SalesForce.com يكون في شكل ويب.

بدلاً من التطبيقات الفردية، والمسـتقلة، فـإن تطبيقات خدمات الويب تكون مختلفة، حيث تتصل مكونات التطبيق بعضها مع بعض عبر شـبكة الإنترنت، وتتصل أيضاً مكونات التطبيـق مـع مكونات تطبيقات أخرى باسـتخدام برتوكولات الاتصـالات المفتوحة. فهي عبارة عن مكونات قائمة بذاتها وتصف نفسـها ويمكن استخدامها من قبل تطبيقات أخرى. وبات شـبه مؤكد أن المديرين سـيواجهون أعداداً متزايدة من تطبيقـات خدمات الويب في المسـتقبل، حيث سـيتم وضع العديد من المـوارد المختلفة فيما نطلق عليه "سـحابة" تقنية المعلومـات IT Cloud، وهي بمثابة توصيلات تخزينية للعديد من الملفات ومصادر البيانات وغيرها من المواد. ويمكن للمرء أن يتطرق بفكره إلى محرك البحث جوجل، عندما ننظر في هذا المفهوم السـحابي، حيث يسـتطيع المسـتخدم الحصول على واحد من العديد مـن نماذج البحث الناتجة بغـض النظر عن مجال موضوع البحـث المطلوب. وقد تكون تطبيقات خدمات الويب مرتبطة بسـحابة الإنترنت تلك فضلاً عن موارد التخزين الخاصة بها مع الوصلات القائمة مع النظم المحلية، سواء كانت شبكات محلية أم لاسلكية. وقد تم الحديث في الفصل التاسـع من هذا الكتاب عن المفهوم الشامل للحوسبة السحابية عندما تم تطبيقها على حوكمة تقنية المعلومات.

شكل توضيحي (١٣-٥)

نموذج تطبيقات خدمات الويب



قد تتكون بيئة SOA في المؤسسة هذه الأيام إما من بيئة نظم كاملة مطبقة بشكل كبير أو مــشروع تطوير لتحويل بعض التطبيقات القائمــة حالياً أو الجديدة إلى SOA. وكلاهما يواجه بعض المخاوف الرئيســية الخاصة بضوابط الحوكمة. وسيحتاج كبار المديرين الذين لديهــم إلمام بالضوابط العامة لتقنية المعلومات التي تتبع نهجاً تقليدياً بشــكل كبير لنظم تقنية المعلومات، إلى إعادة التفكير بتلك الأســاليب المســتخدمة في المراجعة. ووفقاً لمثالنا الســابق حول قطــع لعبة الليغو، فإننا بحاجــة إلى مراجعة الضوابط وإجــراءات الحوكمة المتعلقة بهذه المكونــات العديدة المنفصلة، متضمناً ذلــك الضوابط والصلاحيات المحيطة بكل مكون على حدة وكذلك الروابط فيما بينهم.

ربمــا تكون القضية الرئيســية لحوكمة تقنية المعلومات في بيئــة SOA هي الحاجة إلى مخطط SOA شامل يغطي جميع عناصر الخدمات المتفق والموافق عليها من قبل الأطراف المشــاركة. إن تلــك الاعتبارات الخاصة بوحدات الخدمة تذهــب غالباً إلى ما هو أبعد من مجرد قسم تشغيل بل إلى ما هو أبعد من المؤسسة بأكملها فقد تصل إلى مزودي أو موردي خدمــات آخرين. لذا فإن هناك حاجــة إلى نظام قوي للصلاحيات وإلى ضوابط بداخل كل عنــصر مــن عناصر الخدمات. وبالعودة مــرة أخرى إلى مثالنا الــذي يتحدث عن قطع أو وحــدات لعبة الليغو، فكل وحدة خدمية يجب اعتبارها واحدة من قطع هذه اللعبة التي ربمــا تكون عبارة عــن مزيج من عناصر برمجية وموارد بيانات. ويجب على وحدة الأعمال أن تجعــل العناصر غير المملوكة من قبل أي من هذه القطــع (الوحدات الخدمية) متاحة للوحــدات الأخرى من خلال عمليات إفصاح وصلاحيات واضحة. كما يجب اعتماد وظيفة مهنــدس SOA بدرجة ما للقيام بمراجعة تلك العناصر الخدمية ووضع القواعد والإجراءات الداعمة.

تعد الإجراءات القوية المتعلقة بأفضل الممارسات الخاصة بالبنية التحتية، والتي تحدثنا عنها في الفصل السابع من هذا الكتاب على أنها جزء من معايير الأيزو، من الأمور الأساسية في بيئــة SOA. فلا تتم عملية إطلاق المنصــات الخاصة ببيئة SOA عن طريق تطبيق كل شيء بأســلوب تطبيق الكل مرة واحدة. بل، ســيتم إضافــة أو تعديل أو حذف الخدمات والعمليات بشكل اعتيادي وعلى أساس مستمر. التحدي هنا أكثر تعقيداً بكثير من ضوابط

خاصة بمكتبة برامج مستقلة، بل ستكون المخاوف متعلقة بعنصر برمجي واحد في التطبيق. لذا ففي ظل بيئة SOA، فإن التغيرات التي تطرأ على الوحدة الخدمية التي يمكن أن تكون جـزءاً من العديد من العمليات الأخرى التي ربما لا يسـتطيع صاحب أو مقدم الخدمة أن يفهم تماماً من هو الشـخص الآخر الذي يسـتخدم هذه الوحدة الخدمية. وعلى ذلك فقد يكون لمشـكلة التحكم بخدمة واحدة آثار على العديد من الآخرين. لذا فإن هناك حاجة إلى ضوابط قوية في الفحص والجودة.

إن العديـد من الإجـراءات العامة لحوكمة تقنية المعلومـات التي تم الحديث عنها في فصول أخرى من هذا الكتاب يمكن تطبيقها أيضاً في بيئة SOA. على سبيل المثال، الضوابط الداخلية لإطار العمل COSO التي تمت مناقشتها في الفصل الرابع وضوابط حوكمة تقنية المعلومات الخاصة بإدارة أمن وسرية المعلومات التي تمت مناقشـتها في الفصل العاشر من هـذا الكتـاب ملائمين تماماً في بيئة SOA. وعلى الرغم من أن هذه الضوابط الأخرى ملائمة لبيئات مختلفة، فإن الشـكل التوضيحـي (١٣-٦) يوجز الضوابـط الخاصة بحوكمة تقنية المعلومات في بيئة SOA. إن هذه الخطوات الإجرائية تتحدث عن بيئة لم تصل المؤسسـة فيهـا بعد إلى درجة التناغم مع بيئة SOA بنسـبة ١٠٠٪، ولكنها تتحرك باتجاه بيئة SOA من خلال مشروع تطبيقي مستمر وفقاً لمخطط متفق عليه.

لقـد ناقش هذا الفصل بيئة SOA كما لو كانـت مجموعة خاصة من عمليات حوكمة تقنية المعلومات. ومع ذلك، فإننا عندما نقوم بتحريك نظم وعمليات تقنية المعلومات أكثر وأكثر باتجاه بيئة خدمات شـبكة الويب، حيث ستصبح عمليات SOA هي المعيار وليست الاسـتثناء. لذا فالمديرون بحاجة إلى التفكير بنظم وعمليات تقنية المعلومات الخاصة بهم وفقاً لنموذج بيئة SOA.

شكل توضيحي (١٣-٦)

الضوابط الخاصة بحوكمة تقنية المعلومات في بيئة SOA

١. هل قامت المؤسسة بتطوير إستراتيجية شاملة لبيئة SOA تخص تقنية المعلومات وعمليات التشغيل الخاصة بأعمالها، والموافقة عليها؟
أ. إذا كانت هناك إستراتيجية معتمدة، هل تم تنفيذها بالكامل؟ أو ما مدى اكتمالها في الوقت الحالي؟ ب. إذا لم يكن هناك خطة إستراتيجية رسمية لبيئة SOA، فما الخطط المستقبلية لتنفيذ هذا الأمر؟ ج. هل توجد برامج تعليمية تم تقديمها لتوضيح فوائد بيئة SOA العائدة على كل من الأعمال ومستخدمي تقنية المعلومات؟
٢. هل تم تعيين المدير المسؤول عن قيادة وتنسيق الأعمال والجهود المبذولة في بيئة SOA في المؤسسة؟
٣. هل حصلت المؤسسة على أي من برمجيات SOA أو قامت بتقييمها؟ أ. هل تم وضع معايير تقييم رسمية لاختيار البرمجية المناسبة؟ ب. بالنسبة لأي برمجية معمول بها، هل كان هناك برنامج فحص وتقييم رسمي لتحليل المنتج البرمجي فيما يخص التطبيق الكامل؟
٤. هل تم تحديد تطبيقات "الأعمال الحساسة" على أنها جزء من إستراتيجية SOA؟ أ. بالنسبة للتطبيقات الحساسة التي لا زالت غير قائمة على خدمات شبكة الويب، هل يوجد هناك مخططات موضوعة موضع التنفيذ لتحويلها إلى بيئة SOA؟ ب. هل تم تعريف وتوثيق طبقة عمليات الأعمال الحساسة بشكل رسمي لتطبيقات بيئة SOA؟ ج. هل هناك دليل على أن طبقة خدمات التطبيقات تركز على تكامل التشغيل الداخلي، ومعتمدة على قاعدة البيانات، والمكونات، والبنية التحتية؟
٥. هل تم تكوين فريق رسمي لإدارة أو قيادة خدمات SOA؟ أ. هل تمت مراجعة الأهداف والمخاطر الخاصة بمدير الخدمة مع الإدارة؟ ب. هل تم شرح ومناقشة خطط المؤسسة الخاصة ببيئة SOA مع الأعضاء الرئيسيين في فريق الإدارة؟

٦. هل هناك دليل على أن خطط SOA متكاملة تماماً مع خطط استمرارية الأعمال في المؤسسة؟
٧. نظراً لأن المؤسســة تتجه نحو بيئة SOA، فهل تمت عملية التحويل الأوَّلي للتطبيقات من وضعها التقليدي إلى بيئة SOA على أساس الفحص؟ أ. كجزء من أي تحول تجريبي إلى بيئة SOA، هل تمت مراجعة وتقييم ضوابط التطبيقات القائمة حالياً؟ ب. هل يشــتمل أي جزء من عملية تحويل تطبيق ما إلى بيئة SOA على فحص للســمات الخاصة بمكونــات "التوصيل والتشــغيل" Plug and Play والتــي تعد من الفوائــد المفترضة للعمليات التشغيلية لبيئة SOA؟ ج. هــل هنــاك دليل على أن التكاليف والفوائد الناجمة عــن أي عملية تحويل لبيئة SOA قد تم تقييمها رسمياً؟
٨. بناء على الفحوصات والتقييمات، هل جميع التطبيقات المحولة لبيئة SOA متسقة مع المتطلبات الأمنية الخاصة بتطبيقات ونظم تقنية المعلومات المؤسسية؟
٩. عــلى أســاس الاختبارات، هل تــم وضع إجراءات واســتيعابها من قبل كل مــن تقنية المعلومات والمديرين المسؤولين عن التطبيقات المحولة إلى بيئة SOA؟
١٠. هــل تــم تحديد وتقييم للتكاليف والفوائــد الناجمة عن أي تحويل لبيئــة SOA قبل عمل أي تحويلات مخطط لها على نطاق واسع؟

ملاحظات:

١. ليجو LEGO اســم علامة تجارية لعدد كبير من عناصر البناء وأي شكل من أشكال الألعاب في أشكال وألوان مختلفة، والتي يمكن توصيلها معاً لخلق هياكل مختلفة للألعاب، ومن ثم تفكيكها بســهولة لخلق شيء آخــر. هذا المنتج من ألعاب الأطفال متاح في جميع أنحاء العالم. فهو نموذج جيد للبناء من خلال تركيب المكونات. مزيد من المعلومات يمكن العثور عليها في الموقع www.LEGO.com.

٢. إطــار عمل نت. (Net.) أو دوت نت عبارة عن نموذج برمجة شــامل ومترابط لبناء التطبيقات. www.microsoft.com/net.

٣. بيــا BEA هو أحد وحدات شركة أوراكل. يمكــن العثور على معلومات عن تطبيق الويب لوجيك WebLogic الخاص به في موقع www.oracle.com/bea/index.html

الفصل الرابع عشر
إدارة تهيئة ومحفظة تقنية المعلومات

إن أي نظام تقنية معلومات مثبت، سواء كان جهاز حاسب لوحي أم حاسباً آلياً محمولاً خاصــاً بأحد المديريــن أو نظاماً خادماً داعماً لمكتب مبيعات أحــد الفروع أو مركز بيانات رئيســياً لإحدى الشركات؛ ســيكون به العديد مــن المكونات التي تشــمل محافظ البرامج التطبيقية والملفات وقواعد البيانات ونظم التشغيل وأجهزة الاتصال ووثائق الدعم الخاصة بهــذه الإجــراءات. وينبغي أن تكون كل هذه المكونات مترابطــة بين جميع الأنظمة وعبر المؤسسة بأكملها لكي تكون قادرة على الاتصال والعمل بعضها مع بعض. ويطلق على هذا التجميع الكامل لمكونات تقنية المعلومات اسم تهيئة تقنية المعلومات IT Configuration في المؤسسة. وكأحد العناصر الهامة في حوكمة تقنية المعلومات، فإنه ينبغي أن يكون هناك عمليــات معمول بهــا لإدارة التوافق بين مكونات هذه التهيئة لتقنيــة المعلومات وحالتها كالتأكــد من قدرة هذه المكونــات على التحدث والتواصل معاً. لذا ينبغي على المؤسســة أن تمتلــك نظاماً فعالاً لإدارة تهيئة تقنية المعلومات، وذلك لدعم عمليات تقنية المعلومات الرئيسية لديها.

يتعــرض مديرو الأعمال غالباً إلى مســائل تتعلق بتهيئة تقنيــة المعلومات عندما يتلقون بلاغاً أو رســالة خطأ من إحدى إدارات المؤسســة التابعين لها ويكتشــفوا أنه ليس بإمكانهم قــراءة الملف الذي تم إرســاله. وتكون أول ردة فعل للمدير الاتصــال بـفريق الدعم الفني التابع لإدارة تقنية المعلومات التابعة له أو لها، وفي الغالب يتم تتبع المشــكلة لنكتشــف أن الوحدة التي قامت بإرسال البيانات التي لا يمكن قراءتها قد قامت باستخدام أحد الإصدارات الخاطئــة للبرمجية أو حتى أنها قد اســتخدمت برمجية غير صحيحــة بالمجمل. وفي الغالب يكون سبب مشكلة تلك البرمجية الخاطئة أو غير القابلة للقراءة هو الإخفاق في تحديث أحد عناصر البرمجية في مكان ما في شــبكة تقنية المعلومات الخاصة بالشركة. فقد يكون التقرير أو العملية جيداً في الموقع الذي يتم تشغيلها فيه حالياً، ولكنها غير متوافقة مع نظم وأجهزة أخرى. ويعد هذا أحد الأمثلة على المشاكل المتعلقة بتهيئة تقنية المعلومات!.

هنـاك حاجة للمحافظـة على إعـدادات ثابتة ومتوافقة بـين الموارد الخاصـة بتقنية المعلومات، سـواء كانت ملفات بيانات وبرامج محملة على جهاز حاسـب شخصي محمول أو على موارد موجودة في مكان ما في شـبكة تقنية المعلومات الخاصة بالشركة. إذا حدث تغيـير أو تعديـل على أحد المكونات يكـون هناك غالباً حاجة لانعـكاس ذلك على جميع المكونـات الأخرى المترابطة معه. وتُعـرف الإدارة الخاصة بمراجعات تلك العناصر العديدة لتقنيـة المعلومات وإصداراتها باسـم إدارة تهيئـة تقنية المعلومـات IT configuration management. وينظـر إلى هـذا المجال غالباً على أنه مجـرد رقابة فنية فقط على تقنية المعلومات، في حين أنه يجب أن ينظر للإدارة الفعالة لتهيئة تقنية المعلومات على أنها أحد المكونات الهامة والضرورية لحوكمة تقنية المعلومات.

يناقش هذا الفصل أهمية عمليات إدارة تهيئة تقنية المعلومات في كل المؤسسات ويوجز الأدوات الرئيسية لحوكمة تقنية المعلومات اللازمة لإيجاد نظام فعال لإدارة التهيئة الخاصة بالمؤسسـة Configuration Management System (CMS) مـع التركيز على إنشـاء ما يسمى قاعدة بيانات إدارة التهيئة Configuration Management Database (CMDB). وقد تم تسـليط الضوء على بعض عناصر عمليات إدارة تقنية المعلومات في الفصل السادس من هذا الكتاب الذي كان يدور حول أفضل الممارسات الخاصة بآيتل وإدارة خدمات تقنية المعلومـات، إلا أن هذا الفصل يؤكد مرة أخرى أهمية إدارة تهيئة تقنية المعلومات بوصفها أحد الضوابط الهامة لحوكمة تقنية المعلومات.

كـما سـيقدم ويناقش هذا الفصل أيضـاً إدارة محفظة تقنية المعلومـات على أنه أحد المفاهيـم الهامة في حوكمة تقنية المعلومات. وكما هو الحال بالنسـبة للعديد من الأفراد الذين يستثمرون في أحد صناديق الاستثمار التعاونية أو في أحد صناديق التداولات التجارية للبورصة الذي يحتوي على محفظة أوراق الاسـتثمار المالية ذات العلاقة، فهناك مزايا قوية لحوكمة تقنية المعلومات نتيجة إدارة موارد تقنية المعلومات، وذلك استناداً إلى مجموعات أو محافـظ التطبيقـات والبنية التحتية والمشـاريع وموارد تقنية المعلومـات ذات الصلة. وسـوف نصف هنا كيف يمكن لنهج إدارة محفظة تقنية المعلومات الخاصة باسـتثمارات تقنية المعلومات أن يؤدي إلى العديد من الفوائد لصالح إدارة تقنية المعلومات والمؤسسـة بكاملها. وتعتبر إدارة محفظة تقنية المعلومات واحدة من الطرق الفعالة لإدارة استثمارات

تقنيــة المعلومات والتي يمكن أن توفر رقابة مركزية على ميزانيات تقنية المعلومات وقضايا إدارة مخاطر تقنية المعلومات والتوافق الإســتراتيجي لاستثمارات تقنية المعلومات. فإدارة محفظة تقنية المعلومات تسهم في دعم ممارسات محسنة لحوكمة تقنية المعلومات.

مفاهيم إدارة تهيئة تقنية المعلومات:

يوجد العديد من المعدات والبرمجيات ومكونات البنى التحتية الخاصة بتقنية المعلومات في أي نظام من أنظمة تقنية المعلومات المؤسســية. وهي تمتد من خادم قواعد بيانات مع مجموعــة من الأجهزة الطرفية المتصلة به والتي تســتطيع أن تخــدم وحدة أعمال صغيرة وصولاً إلى مجموعة كبيرة من عمليات تشــغيل تقنية المعلومات على مستوى الشركة والتي تخدم مرافق مختلفة في جميع أنحاء العالم. بعض هذه المكونات تكون مترابطة فيما بينها، في حــين أن البعض الآخر يكــون قائماً بذاته ومنفصلاً عن باقي المكونــات. إن تهيئة تقنية المعلومات في المؤسســة تعد أكثر من مجرد قائمة من المكونات البرمجية والأجهزة والمعدات المثبتــة. بل يجب على الســجلات الخاصة بالتهيئة أن تحتفظ بأمــور مثل روابط الواجهة والتعريفــات الخاصة بإصدار المكون والخصائــص المثبتة وجميع الأمور الأخرى التي تصف تلك العناصر والبنود الخاصة بتهيئة تقنية المعلومات في الحالات التي تم تثبيتها فيها.

لقــد تطرقنا ســابقاً إلى مفاهيم إدارة تهيئــة تقنية المعلومات في الفصل الســادس من هــذا الكتاب والذي يدور حول إطار العمــل آيتل والمفاهيم الخاصة بـإدارة خدمات تقنية المعلومــات. كانت إدارة تهيئة تقنية المعلومات هناك عبارة عن عنصر واحد فقط من بين سلســلة من الممارسات الجيدة للإطار آيتل. في حين أن هذا الفصل ينظر بعمق أكبر بقليل إلى أدوات وعمليــات إدارة تهيئة تقنية المعلومات. وســيوضح هذا الفصل لماذا تعد إدارة تهيئة تقنية المعلومات أحد المكونات الهامة للعمليات الرشيدة لحوكمة تقنية المعلومات.

وعــلى الرغم من عدم وجود أي تعريــف موحد أو متفق عليه لنظام إدارة تهيئة تقنية المعلومــات، حتــى إن البحث عن طريق شــبكة الإنترنت ســوف يعطي أيضــاً العديد من التعريفات المختلفة، فإن المنظمة التقنية لوضع المعايير والتي مقرها الولايات المتحدة، وهي IEEE، تعد من المصادر الجيدة للحصول على مثل هذا التعريف. وقد كانت هذه المنظمة

تُعرف سابقاً باسم جمعية مهندسي الكهرباء والإلكترونيات Institute for Electrical and Electronic Engineering. ويشــار إليها حالياً باستخدام الأحرف الأولى من اسمها حيث أصبــح الاســم الدارج لها هــو IEEE " آي تريبل إي". حتى الموقــع الخاص بهذه المنظمة www.ieee.org لا يشــير إلى الاســم الأصلي الكامل لها. وتُعَرِّف منظمة IEEE إدارة تهيئة تقنيــة المعلومات على أنها إحدى العمليات الخاصة بالمؤسســة أو بإدارة تقنية المعلومات، حيث تحتوي هذه العملية على العناصر التالية:

- **التعريف:** تشتمل عملية إدارة تهيئة تقنية المعلومات على مخطط تعريفي قوي يعكس بنيــة جميع موارد تقنية المعلومات، ويحدد مكوناتها وتاريخ التعديل وأنواع هذه الموارد. الأمر الذي يجعل هذه الموارد مميزة ويمكن الوصول إليها بشكل أو بآخر.
- **التحكــم:** يتعين عــلى نظام إدارة تهيئة تقنية المعلومــات التحكم في الإصدارات الخاصة بـجميع المنتجــات والتغيرات التي تحدث على الموارد الخاصة بالتهيئة طوال دورة حياتها من خلال وجود ضوابط معمول بها تضمن تناغم الموارد الخاصة بمكونات تقنية المعلومات من خلال وضع ما يعرف بمنتجات الخط المرجعي baseline products.
- **تدوين الحالة:** يجب على نظام إدارة تهيئة تقنية المعلومات أن يســجل ويبلغ عن حالة كل مكون من مكونات بنية تقنية المعلومات وطلبات التغيير، وذلك أثناء جمع المعلومات الإحصائية الحيوية المتعلقة بتلك المكونات الموجودة في منتجات التهيئة.
- **التدقيــق والمراجعة:** ينبغي أن تكــون هناك عمليات مراجعة معمول بها تقوم بها إدارة تهيئــة تقنية المعلومات للتحقق من ســلامة اكتمال جميع بنود تهيئــة تقنية المعلومات والحفاظ على التوافق فيما بين المكونات المترابطة بداخل التهيئة من خلال ضمان أن هذه المنتجات هي عبارة عن مجموعة من المكونات المعرفة على نحو جيد.

سوف تناقش الفقرات التالية تلك العناصر الخاصة بإدارة تهيئة تقنية المعلومات ونظام إدارة التهيئة CMS بمزيد من التفصيل. فللوصول إلى إدارة فعالة لتهيئة تقنية المعلومات، فإنه يتعين على المؤسســة وإدارة تقنية المعلومــات التابعة لها (١) امتلاك عمليات معمول بهــا لتحديد جميع المكونات الخاصة بالأجهزة والبرمجيات والبنية التحتية، والتي تعد جزءاً مــن موارد تقنية المعلومات لديهــا. (٢) امتلاك ضوابط معمول بهــا لمتابعة كل التغيرات

والتنقيحات التي تتم على هذه المكونات الخاصة بتهيئة تقنية المعلومات. (٣) الإبقاء على نظام تبليغ خاص بإدارة التهيئة بحيث يكون كل من إدارة تقنية المعلومات والإدارة العامة والمــوارد المالية على دراية بالوضع الراهن لموارد تقنية المعلومات الخاصة بالمؤسســة. (٤) متابعة وإدارة حالة تلك الموارد الخاصة بتقنية المعلومات للتأكد من أنها قائمة، وفعالة من حيث التكلفة.

إن الإدارة الفعالــة لتهيئة تقنية المعلومات هي أكثر بكثير من مجرد التحكم بإصدارات البرامــج الخاصة بتقنيــة المعلومات من خلال قاعدة بيانات واحدة وشــاملة لإدارة التهيئة CMDB، بل قد تشــمل أيضاً موارد أخرى ذات صلة موجودة في أحد المرافق كإدارة تقنية المعلومات الموجودة في المقر الرئيسي للمؤسســة. كما يجب أن تشمل عمليات إدارة تهيئة تقنية المعلومات كامل المؤسســة متضمناً ذلك أي مرفق قد تكون هناك حاجة للاتصال به أو مشاركة البيانات والمعلومات معه.

لقــد تحدثنا عن الممارســات الخاصة بإدارة تهيئة تقنيــة المعلومات التي تعد جزءاً من الإطار آيتل والذي ســبق الحديث عنه في الفصل الســادس من هــذا الكتاب. ولأن أفضل الممارسات الخاصة بالإطار آيتل تغطي مجموعة كبيرة من المجالات، يجب إعطاء المزيد من الاهتمام بإرشــاداتها المتعلقة بإدارة تهيئة تقنية المعلومات. تقدم الأجزاء القادمة من هذا الفصل المزيد من الإرشــادات فيما يتعلق ببناء العمليات الخاصة بتهيئة تقنية المعلومات. يصــف الشــكل التوضيحي (١٤-١) هــذا المفهوم الخاص بــإدارة التهيئة CMS كما يصف الحاجة إلى ضوابط خاصة بتهيئة تقنية المعلومات. يعرض الرســم البياني مســتخدمي نظم الأعــمال المؤسســية في الإطار الدائري الخارجــي له، حيث إن جميعهــم بحاجة إلى إيجاد علاقات وروابط فيما بينهم من خلال موارد النظم الخاصة بهم. ويهتم هؤلاء المستخدمون للنظم بالقضايا الآتية والمتعلقة بتهيئة تقنية المعلومات:

- **ضوابط أصول تقنية المعلومات:** قد تَعْمَد المجموعات المختلفة للمســتخدمين وإدارات تقنية المعلومات إلى شراء وتثبيت إصدارات مختلفة بعض الشيء من البرمجيات والأدوات. وفي بعــض الأحيــان تكون الاختلافات بشــكل عام قليلــة، فمثلاً قد يكــون لدى إحدى الوحدات خارج البلاد إصدار مختلف بعض الشيء بسبب اختلافات اللغة. على كل حال،

قــد تختلف الطريقة التي تفسر فيهــا البرمجية الأوامر وتتفاعل من خلالها مع إصدارات اللغــات الأخرى. وقــد تثير الكيفية التي تقوم من خلالها المؤسســة ووحدات العمليات التشــغيلية التابعة لها بشراء وتثبيت البرمجيات والأصول الأخرى لتقنية المعلومات بعض القضايا المتعلقة بعملية التهيئة.

- **إدارة الحوادث:** إن الهدف الأول لعملية إدارة الحوادث هو اســتعادة عملية التشــغيل الطبيعية للخدمة بأقصى سرعة ممكنة وتقليل التأثير على العمليات التشــغيلية للأعمال. هذا من شأنه أن يضمن الإبقاء على أفضل المستويات الممكنة فيما يتعلق بجودة الخدمة وإتاحتها. من ناحية أخرى، قد تغفل النشاطات التصحيحية للحوادث الطارئة عن روابط أو اتصالات في التهيئة، مسببة بذلك مشاكل عامة على المدى التشغيلي البعيد.
- **إدارة مشــاكل تقنية المعلومات:** يُعَرِّف الإطار آيتل المشكلة على أنها حالة يتم تحديدها غالبــاً نتيجة لحــوادث متعددة تُظْهِر أعراضاً مشــتركة. فعندما يتعــرض أكثر من نظام أو مجموعة مســتخدمين للمشكلة التقنية نفســها، فإن هناك حاجة للوصول إلى المصدر الرئيسي المســبب للمشــكلة وتحديد الحل المناســب لها. فقد يصبح هذا أحد المشاكل الكبيرة في التهيئة في البيئات الكبيرة والمعقدة لتقنية المعلومات.
- **القضايا الشــاملة لحوكمة تقنية المعلومات:** لقد تم تغطية مجموعة واســعة من قضايا حوكمة تقنية المعلومات خلال فصول هذا الكتاب، والتي تشــمل السياســات الأمنية في تقنية المعلومات وقضايا إدارة المشــاريع والمقاييــس المعيارية وغيرها. لذا يجب أن يتم تنفيذ وإدارة كل هذه الأمور بشــكل متناغم عبر المؤسســة لضمان إدارة متسقة وفعالة للتهيئة.
- **إدارة ســعة تقنية المعلومات:** تحتاج المؤسســة إلى تثبيت وتنفيذ المســتويات والأحمال الصحيحــة لموارد تقنية المعلومات. لذا فإن معالجة احتياجات وأحجام الخدمات بحاجة إلى متابعة وضبط عبر جميع موارد تقنية المعلومات في المؤسسة.
- **اتفاقيات مســتوى الخدمة SLAs:** التي تــم تقديمها مع قضايا حوكمة تقنية المعلومات التي تمت مناقشــتها في الفصل الســابع عشر من هذا الكتاب. هي عبارة عن اتفاقيات غير رســمية تعقدها إدارة تقنية المعلومات مع كل من مجتمعات المســتخدمين التابعين

لها والموردين الخارجيين. أبســط صور هــذه الاتفاقيات، أن تقوم إدارة تقنية المعلومات بوضع اتفاقية لمســتوى الخدمة مع قسم المراقبة المالية بحيث يتعهد المحاسبون بتسليم جميع معاملات إغلاق نهاية الشهر الخاصة بدفتر الأستاذ العام وفقاً لجدول زمني متفق عليه على أن تتعهد إدارة تقنية المعلومات باســتكمال وتسليم تقارير الإغلاق الشهرية في تاريــخ محدد. من ناحية أخرى عندما تحتاج جميع الإدارات المختلفة إلى المســتخدمين ومرافق تقنية المعلومات لاتفاقيات مستوى خدمة خاصة بها، قد تكون هناك مشاكل في نظام إدارة التهيئة CMS.

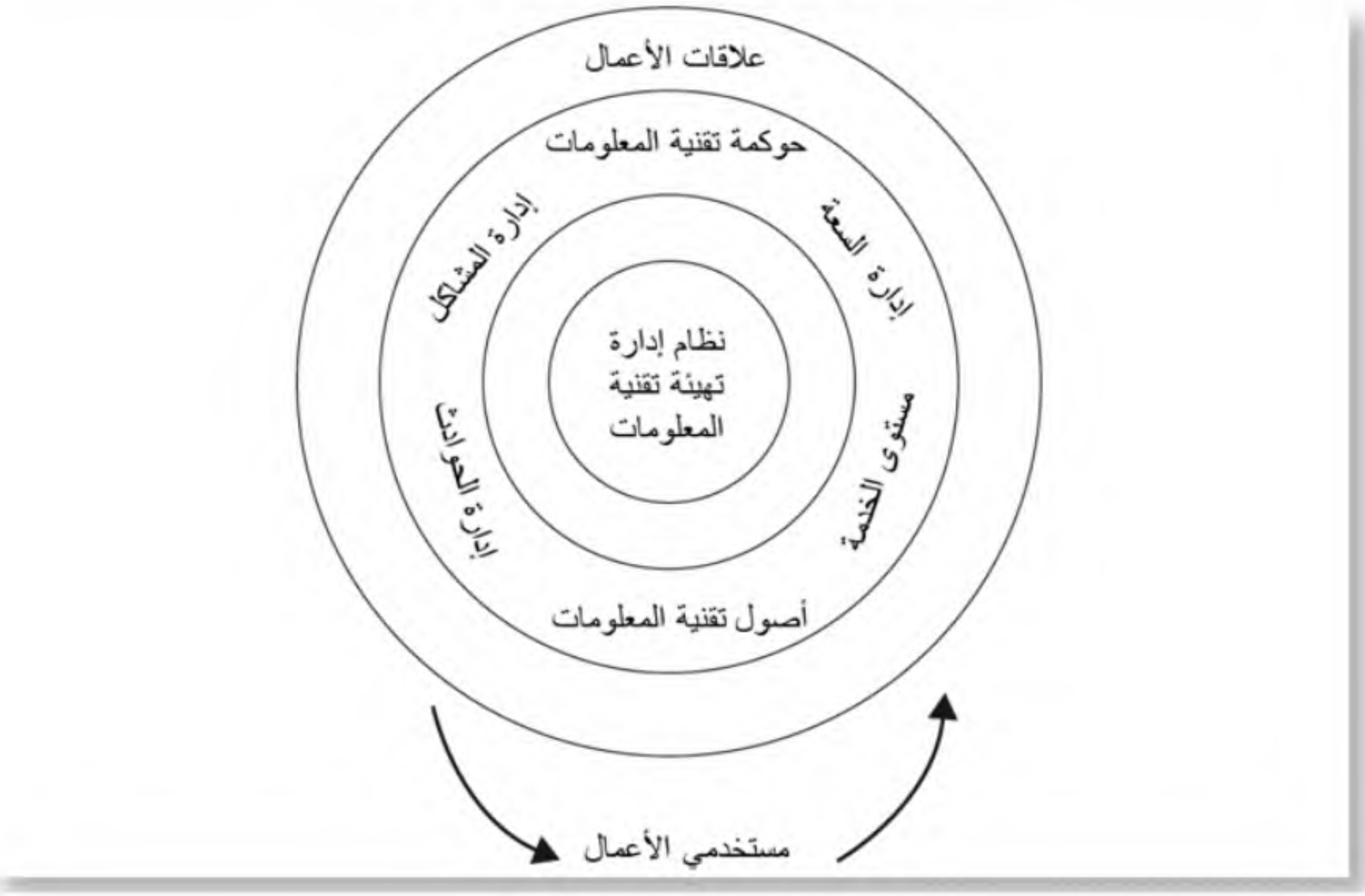
الفكــرة هنا هو أننا يجب أن ننظــر إلى إدارة تهيئة تقنية المعلومات على أنها مجموعة مــن المفاهيــم التي تكون منفصلة غالبــاً لكنها مترابطة (انظر الشــكل التوضيحي ١٤-١). ويعــد هذا من الأمور الهامــة خصوصاً هذه الأيام؛ إذ إننا قد ابتعدنا كثيراً عن الحاســبات المركزية التي كانت موجودة في الماضي وقمنا بتثبيت أشكال وأنواع عديدة من موارد تقنية المعلومات في المؤسسة التقليدية ذات الوحدات والمواقع المتعددة. وبينما يجب على الإدارة التقليدية لتقنية المعلومات أن تضع معايير على ما تمتلكه (نظم وعمليات تقنية المعلومات) وكذلــك على نظم وعمليات تقنيــة المعلومات الخاصة بالمقر الرئيسي، فإننا نجد أن ضوابط التهيئة قد تضيع في عالم النظم اللاسلكية المتصلة بالنظم السحابية.

أفضل ممارسات إطار آيتل الخاصة بإدارة تهيئة تقنية المعلومات:

قدم الفصل الســادس من هــذا الكتاب المــواد الخاصة بمكتبة البنيــة التحتية لتقنية المعلومــات ITIL فيما يتعلق بالحوكمة، وقد تم هناك عرض أفضل الممارســات بالشــكل التوضيحــي (٦-٢) موضحــاً أهميــة إدارة التهيئة عــلى أنها إحــدى أدوات حوكمة تقنية المعلومات. الفكرة هي أن كل مؤسســة تمتلك أو تحتفظ بعناصر متنوعة من المعلومات عــن البنية التحتية الخاصة بتقنية المعلومات لديها، فضلاً عن أن المؤسســة، تواجه تحدياً بالنسبة لعملية الحفاظ على النسخة الأخيرة المحدثة لجميع هذه المعلومات. وقد حددت إدارة التهيئــة في الإطــار آيتل أفضل الممارســات للاحتفاظ بتفاصيــل المعلومات الموثوقة والحديثة المتعلقة بالبنية التحتية لتقنية المعلومات.

شكل توضيحي (١٤-١)

مفاهيم نظام إدارة تهيئة تقنية المعلومات



مع أن هذا المصطلح لا يعد من المصطلحات الشائعة الاستخدام بالنسبة للعمليات التشغيلية الخاصة بتقنية المعلومات هذه الأيام، فإن إطار العمل آيتل يدعو المؤسسة والعمليات التشغيلية الخاصة بها إلى تعريف هيكل التهيئة الخاص بها إلى ما يطلق عليه الإطار آيتل عناصر التهيئة Configuration Items (CIs)، كما يدعو الإطار آيتل أيضاً إلى أن نفهم كيف ترتبط عناصر التهيئة CIs هذه بعضها مع بعض. كما يجب على العملية الفعالة لإدارة التهيئة في آيتل أن تؤكد أن التغيرات التي حدثت على بنية تقنية المعلومات قد تم تسجيلها بشكل صحيح، بما فيها العلاقات بين عناصر التهيئة CIs. كما يجب على عملية إدارة التهيئة مراقبة حالة مكونات تقنية المعلومات لضمان أنها تملك الوصف الدقيق للإصدار الحالي لتلك العناصر CIs.

وفي خطوة أولى لبناء عمليات التهيئة الفعالة لتقنية المعلومات، فإن المؤسسة تحتاج إلى القيام بجرد موارد تقنية المعلومات الموجودة لديها. فهذه العملية تحتاج إلى ما هو أكثر من

مجرد مســح لقوائم المكونات البرمجية المثبتة وعمل الجرد المادي لمعدات تقنية المعلومات الموجودة على الأرض. يحتوي الشكل التوضيحي (١٤-٢) على قائمة بأنواع الموارد التي يجب أن تصبح من عناصر التهيئة CIs لتحديد بيئة التهيئة، وبمثابة اللبنات الأولى في قاعدة بيانات إدارة التهيئة CMDB كما ســيتم مناقشــته في الأجزاء اللاحقة. وعنــد تنفيذ الجرد بصورة فعالــة، فإنه يجــب أن يُزَوِّد هذا الجرد كلاً مــن الإدارة وإدارة تقنية المعلومات بالمعلومات والمجالات لمزيد من التحقيق في المجالات التالية والخاصة بسياسة منتجات تقنية المعلومات:

- ما مكونات تقنية المعلومات المســتخدمة حالياً؟ وكم عدد الإصدارات المختلفة المعمول بها لكل مكون؟ وما المدة التي استخدمت فيها هذه المكونات؟
- ما المكونات التي يمكن أن يتم سحبها تدريجياً؟ وما المكونات التي تحتاج إلى تعديل؟
- ما التراخيص المفعلة؟ وهل هي كافية؟
- ما مدى معيارية البنية التحتية الشاملة لتقنية المعلومات عبر المؤسسة؟

شكل توضيحي (١٤-٢)

أمثلة على عناصر التهيئة الموجودة في قاعدة بيانات إدارة التهيئة CMDB

• جميع منصات الحوسبة المادية وتشمل أجهزة الحاسب المكتبي والحاسب المحمول والخوادم المثبتة على حامل rack-mounted والخوادم النحيفة Blade servers وأجهزة أخرى قائمة بذاتها.
• جميع أجهزة ومعدات الشبكة متضمنة الطابعات المتصلة بالشبكة.
• جميــع التطبيقــات والبرامــج الخدميــة Utilities الخاصــة بالبرمجيات الوســيطة Middleware والبرمجيات Software متضمنة المنتجات الخاصة بالمستخدم النهائي، والإدارة والدعم.
• جميع نظم التشغيل المثبتة وكذلك أدوات حزم تطوير البرمجيات مثل جافا JAVA وسي شارب C# وأدوات البرمجيات الإدارية الخاصة بدورة حياة تطوير النظم SDLC.
• تنصيبات الرقع Patches الخاصة بأنظمة التشغيل وأجهزة الشبكة.
• شبكة الهواتف المحلية Private Branch Exchange (PBX) ومعدات وبرمجيات الاتصالات المتعلقة بها.
• خدمات الأعمال المثبتة أو عناصر هذه الخدمات.
• حزم الوثائق الخاصة بالتطبيقات والنظم والمعايير الخاصة بالسياسات والعمليات.

الفكرة هنا هي أن المفاهيم الخاصة بإدارة تهيئة تقنية المعلومات ونظام إدارة التهيئة CMS لا يجب أن تكون مجرد قضايا تابعة لإدارة تقنية المعلومات في المؤسسة. بل يجب تشكيل فريق مكون من المختصين في التقنية يشمل إدارة تقنية المعلومات وغيرهم من المستخدمين الرئيسيين لموارد تقنية المعلومات من أجل بناء وتشييد نظام لإدارة التهيئة CMS في المؤسسة. لذا يجب إعطاء المزيد من الاهتمام من أجل ضم أعضاء لفريق مشروع نظام إدارة التهيئة CMS من أشخاص في المؤسسة لا علاقة لهم بتقنية المعلومات والذين يستخدمون الموارد الأخرى عادة للنظم ولديهم اتصالات محدودة مع نظم المؤسسة الأكثر مركزية. كما يجب أن يحتوي النظام الفعال لإدارة التهيئة على كل مجموعات المعلومات المشار إليها في الشكل.

جمع وتحليل متطلبات إدارة التهيئة:

بينما يدرك العديد من المديرين والعاملين في تقنية المعلومات أهمية امتلاك عمليات خاصة بتهيئة فعالة لتقنية المعلومات ومعمول بها في المؤسسة؛ قد تمثل عملية جمع وتحديد المتطلبات الضرورية للبدء بإدارة التهيئة على مستوى المؤسسة بشكل دقيق ومحدد، أحد التحديات الموجودة. حيث يجب أن تبدأ هذه الممارسة من خلال النظر إلى أدوات التهيئة المعمول بها، وإجراء التعديلات اللازمة عليها حسب الحاجة، ومن ثم بناء علاقات رفيعة المستوى لإدارة التهيئة بحيث تحمل توقعات أكثر واقعية والانتقال إلى متطلبات قابلة للقياس لعملية تهيئة تقنية المعلومات.

إن هذه العملية الخاصة ببناء وإطلاق مكونات إدارة تهيئة تقنية المعلومات وتحديد متطلباتها الضرورية يجب أن تبدأ عادة بالتخطيط ومنح التصاريح وإطلاق مشروع رسمي لتطوير نظم تقنية المعلومات، وذلك وفقاً لمبادئ حوكمة إدارة المشاريع التي سنتحدث عنها في الفصل السادس عشر من هذا الكتاب، فالممارسات القوية لإدارة المشاريع تعد من الأدوات المهمة لإطلاق عملية فعالة لإدارة التهيئة. ويجب أن يتضمن مشروع إدارة تهيئة تقنية المعلومات العناصر الأربعة التالية:

١- **تحديد عناصر تهيئة تقنية المعلومات:** تتطلب هذه الخطوة وضع تعريف شامل لنطاق التهيئة وبيان قائمة بعناصر التهيئة كالموضح بالشكل التوضيحي (١٤-٢)، وكذلك وضع تعريف شامل لعملية تعقب التغيرات، وذلك لإدارة عناصر التهيئة في بيئة تقنية المعلومات.

٢- **بناء العلاقات الخاصة بتهيئة تقنية المعلومات:** يجب ربط عناصر التهيئة CIs المختلفة تلك مع تقنية المعلومات وعمليات الأعمال.

٣- **تحســين عمليات تهيئة تقنية المعلومات:** ربما يجد فريق المشروع أن هناك العديد من عناصر التهيئة CIs مكررة بشكل أساسي بعضها من بعض. ولكن كل عنصر منها موجود في نظــام أو قاعدة بيانــات مختلفة. لذا يجب بذل المزيد من الجهد لتبســيط وتنفيذ هذه العمليات. على ســبيل المثال، يجب أن يتم حفظ أرقام دفتر الأســتاذ العام للنظام المحاســبي في مكان واحد فقط. فالاحتفاظ بقائمة في أماكن متعددة من شأنه أن يقود فقط إلى أخطاء أو مشاكل أخرى ستأتي لاحقاً.

٤- **إيجــاد عمليــات توثيق متســقة لإدارة تهيئة تقنية المعلومات:** ويعــد هذا الأمر أحد المعايــير الهامــة في الحوكمة والتي كانت جزءاً من نقاشــنا الدائر حــول حوكمة تقنية المعلومات في العديد من الفصول.

إن هذه العملية الشــاملة لإدارة التهيئة تشــبه إلى حد ما أي عملية يجب توظيفها عند الحاجة لتنظيم مجموعة كبيرة من عناصر المعلومات المختلفة والمترابطة في الوقت نفســه، مع الحاجة إلى أن نكون قادرين على أن نشير إلى تلك العناصر بانتظام وأن نطبق التغيرات عليها حســب الطلب. ففي حين أن السجلات الشخصية، مثل السجلات الخاصة بإيصالات الضريبة على دخول الأفراد أو ســجلات المنتجات وقطع الغيــار الخاصة بتجار التجزئة يتم تنظيمها عادة ولو على الأقل بصورة غير رسمية شكل من أشكال التهيئة، نجد أن العديد من إدارات تقنية المعلومات تفتقر إلى وجود هذه الأنواع من التطبيقات. فهم يقومون بتثبيت نظم وبرمجيات جديدة، ويعتمدون غالباً على الباعة لتزويدهم بمستوى بسيط من التحكم بالتعديل أو التغيير ولكنهم لا يملكون عمليات معمول بها لإدارة تهيئة تقنية المعلومات.

يتعــين على إدارة تقنية المعلومات في المؤسســة اتخاذ الخطــوات اللازمة لتطبيق إدارة التهيئة على أنها مكون أســاسي لجميع العمليات التشــغيلية لتقنية المعلومات. فمثل هذا العمــل قد يجبر تقنية المعلومات على التراجع عن بعض المشــاريع العادية الأخرى، غير أن العملية الفعالة ســتعود بالفوائد على كل من تقنية المعلومات ومستخدمي خدمات تقنية المعلومات.

خطوات تطبيق إدارة تهيئة تقنية المعلومات:

ينبغـي على إدارة تقنية المعلومات أن تقوم بوضع معايير بشـأن إصدارات البرمجيات والمعـدات الخاصـة بهـا. فالتحكم بالإصدار يكون كممارسـة تهـدف إلى نشر إصدارات برمجيات متوافقة على الأجهزة المتشـابهة داخل الشـبكة. حيث سيسهم ذلك في تحسين فرصة التحقق من صلاحية إصدارات البرمجيات المختارة واختبارها وسـيحد بشـكل كبير من حجم العيوب في البرمجيات ومشكلات التوافق الموجودة على الشبكة. إن الإصدارات المحدودة للبرمجيات من شـأنها أيضاً أن تقلل من مخاطر السـلوك غير المتوقع، وذلك من خلال واجهات المستخدم، والأوامر أو مخرجات الإدارة، وأسلوب الترقية وسلوك الخصائص. هـذا يجعل من البيئة أقل تعقيداً ويجعل عملية تقديم الدعم لها أكثر سـهولة. بشـكل عام، فإن ضبط إصدار البرمجيات يحسـن من إتاحة الشـبكات ويقلل من تكاليف الدعم التفاعلي.

إن الحديـث عن التحكـم بإصدارات مكونات تقنية المعلومات أسـهل مـن القيام به فعلاً. لذا يتعين على العمليات التشـغيلية لتقنية المعلومات في المؤسسـة وفرق البرمجيات المسـؤولة عنها أن تقوم بتعريـف وتحديد تصنيفات للأجهزة اعتـماداً على أنواعها ومدى ثباتهـا ومتطلبات إصدار مزايا جديدة. في المؤسسـات الكبيرة المتعددة الإدارات، لا بد من تثبيت إصدارات برمجيات منفصلة على الأجهزة المتشـابهة. هنا في الغالب يمكن التغاضي عن المعايير. فقد يكون القسم الغربي لمؤسسة ما على سبيل المثال قد نسي أن يثبت بعض التعديـلات الطفيفة على النظم في حين قام القسـم الشرقي من المؤسسـة بتثبيتها. فعلى الرغم من أن النتائج قد تبدو متشـابهة، فإن المسـائل يمكن أن تُنسى إلى أن تتسبب إحدى قضايا النظم بمشاكل مستقبلاً.

ولإيجـاد ضوابط فعالـة لإدارة تهيئـة تقنية المعلومـات، فإنه ينبغي عـلى أخصائيي البرمجيـات أن يقومـوا باختبار إصدارات البرمجيـات والتحقق مـن صلاحياتها وتجربتها. وتتضمن الخطـوات التالية عملية توثيق الإصدارات الناجحـة كمعايير موحدة لتصنيفات الأجهزة المتشـابهة. الفكرة هنا هي نشر وترقية جميع الأجهزة المتشـابهة بشـكل متناغم باستخدام إصدار معياري موحد من البرمجيات.

يعد نظام إدارة تهيئة تقنية المعلومات أحد العناصر الأساسية في الحوكمة الفعالة لتقنية المعلومـات. ففي الواقع لـن نتمكن من إدارة جميع موارد تقنيـة المعلومات الخاصة بنا والتحكم فيها حتى ندرك كيف تتأقلم وتتناسـب هـذه الموارد معاً. إن العنصر الرئيسي في كل هـذا هو الحاجة إلى إيجاد معايير وإجراءات في جميع أنحاء المؤسســة كأن يكون لدى إدارة تقية المعلومات في المؤسســة فهم وإدراك جيد لجميع موارد تقنية المعلومات المثبتة فيها وأنه يجب أن تكون هذه الموارد مرتبطة فيما بينها وأن يتم استخدامها بشكل متناغم ومتوافق عبر المؤسســة. إن التطبيق الفعال لكل من إطار العمل آيتل الذي تمت مناقشته في الفصل السادس من هذا الكتاب، وبيان الخدمات الذي تم الحديث عنه في الفصل الثاني عشر من هذا الكتاب، سـوف يسـهم في تحقيق الوصول إلى هذه البيئة. من ناحية أخرى، فـإن أحد العناصر الهامة في عملية التطبيق الفعـال لإدارة البنية هو تطبيق قاعدة بيانات إدارة التهيئــة CMDB التي تعد بمثابة المكون والمســتودع المركــزي لعمليات إدارة تهيئة تقنية المعلومات.

قاعدة بيانات إدارة التهيئة (CMDB): يكون غالباً مفهوماً صعباً:

قاعــدة بيانــات إدارة التهيئة هي عبارة عــن قاعدة بيانات مفــردة تحتوي على كل المعلومــات المتعلقة بمكونات نظام المعلومات المســتخدم في خدمــات تقنية المعلومات الخاصة بالمؤسســة. بالإضافــة إلى العلاقات الموجودة بين هــذه المكونات. تقدم قاعدة بيانــات إدارة التهيئــة CMDB عرضــاً منظــماً للبيانات، كما توفر وســائل لفحص هذه البيانات من أي منظور نريده. ومن خلال هذا السياق فإن مكونات نظام المعلومات هذا والخــاص بقاعدة بيانات إدارة التهيئة تحتوي عــلى عناصر تهيئة مترابطة وذات مرجعية كما هو موضح في الشــكل التوضيحي (١٤-٢). إن عنصر التهيئة CI قد يكون أي مكون يمكــن تصوره من مكونات تقنية المعلومات متضمنــاً ذلك البرمجيات والمعدات والوثائق والموظفين المسؤولين، بالإضافة إلى أي مجموعة مؤلفة منهم. تسعى عمليات إدارة التهيئة إلى تحديــد وضبــط وتتبع عناصر التهيئــة والتغيرات التي تحدث عليها بطريقة شــاملة ونظامية.

يقـدم العديد من كبار باعة البرمجيات منتجات برمجيـة مختلفة لقاعدة بيانات إدارة المحتوى CMDB. يقدم الشكل التوضيحي (١٤-٣) عرضاً تصويرياً لما يجب أن تظهر عليه قاعدة البيانات تلك أو مكوناتها الرئيسـية. ليس الهدف من هذا الفصل هو تقديم وصف تقنـي حـول كيفية اختيار وبناء قاعـدة بيانات إدارة التهيئـة CMDB، ولكن الهدف هو وصف المكونات الرئيسية لها. وبناءً على الشكل التوضيحي (١٤-٣) فإن قاعدة بيانات إدارة التهيئة يجب أن تحتوي على العناصر والمكونات التالية:

- **إدارة مسـتخدمي قاعـدة بيانـات إدارة التهيئـة CMDB:** باعتبارها أحد النشـاطات المؤسسـية الرئيسـية للتحكـم بقاعدة البيانـات، فإن هنـاك حاجة إلى وجـود واجهة للمسـتخدم والمهام الإدارية. حيث سيكون هذا مزيجاً من الموارد التقنية الخاصة بتقنية المعلومات للمساعدة من خلال الإدارة والمتابعة الشاملة لقاعدة البيانات. هذا بالإضافة إلى توفير عمليـات إدارية لتعريف وإدخال عناصر تهيئة CIs جديدة كلما زاد نمو وتغير النظم والعمليـات. فبالإضافة إلى بناء عناصر التهيئة، فإن هناك حاجة إلى وجود أدوات للاستعلام عن حالات تلك العناصر وتحسين أدائها.
- **أمـن قاعـدة بيانات إدارة التهيئـة وأدوات وصول المسـتخدمين CMDB:** بينما يكون هنـاك حاجـة دائمة لأمن تقنية المعلومـات وأدوات لضبط عمليات الوصـول إليها، فإن المسـألة أصبحت أكثر أهمية فيما يخص قاعدة البيانات الشاملة والضخمة لإدارة التهيئة CMDB. تلـك المنطقـة التي يمكن لشـخص ما فيها أن يحصل عـلى صلاحيات وصول لجميع مصادر بيانات المؤسسة. لذا فوجود ضوابط أمنية قوية يعد من الأمور الأساسية في هذا المجال.
- **الأدوات الخاصـة بإدارة تهيئة قاعدة البيانات:** تعد هذه إحدى الأدوات الخاصة بمجال قواعـد البيانات التي يجب أن تكـون متاحة لتصميم هياكل البيانـات الخاصة بعناصر التهيئة، وذلك لتعزيز فاعلية قاعدة بيانات إدارة التهيئة CMDB. أما الأمر الأكثر أهمية، فهو أن هذا هو المجال الذي يجب أن تكون فيه أدوات الضبط القوية الخاصة بالمراجعة موضوعة في موضع التنفيذ.

- **إدارة البيانات ومســتودع قاعدة البيانــات:** يصف هذا العنصر قاعدة البيانات الفعلية، كما يصف برمجيات التشغيل لها وكذلك الضوابط المادية والبيئية الخاصة بها. لذا هناك حاجة لأخصائيين يتمتعون بمهارات عالية في مجال برمجيات قواعد البيانات لإدارة وضبط البرمجيــات. وبالطبع لا بــد من وجود عمليات صحيحة معمول بها فيما يخص النســخ الاحتياطي واستمرارية الأعمال.
- **ضوابــط أمن وحمايــة البيانات:** كما أن هنــاك احتياجات لضوابط أمــن ووصول قوية معمول بها على روابط واجهة المســتخدم، فــإن هذه العمليات الأمنية تكون أكثر أهمية لأنهــا تعمل مســتودعات من قاعدة بيانــات إدارة التهيئــة (CMDB) وغيرها من نظم الاستخدام الأخرى.
- **مســتودعات تكامل البيانات:** يجب أن يوفر التشــغيل الكامل لقاعــدة بيانات إدارة التهيئة CMDB وصلات إلى مجموعة عريضة من النظم والعمليات. ويعد هذا بمثابة رابط للنتائج الهامة بين قاعدة بيانات إدارة التهيئة CMDB والكيان الكبير للتطبيقات الأخرى.
- **الأدوات الخارجيــة للاكتشــاف والمتابعة:** بالذهاب إلى ما هــو أبعد من قاعدة البيانات الفعلية لإدارة التهيئة CMDB الخاصة بالمؤسســة، فإنه يجب أن يكون هناك مجموعة واســعة مــن الآخرين من الذين لديهــم حاجة للوصول إلى بيانــات CMDB ومراقبتها. فعلى سبيل المثال، قد يحتاج مدققو تقنية المعلومات إلى مراجعة هياكل بيانات محددة وعمليات أخرى ليســت من ضمن عمليات المستخدمين الاعتيادية، ولا حتى من عمليات مسئولي الرقابة.
- **مستودعات بيانات أخرى:** يبين الشكل التوضيحي (١٤-٣) أن قاعدة بيانات إدارة التهيئة CMDB هي بالعادة ليســت المســتودع المركــزي الوحيد لبيانات التهيئة. بل ســيكون هناك أدوات أخرى لقاعدة بيانات التهيئة كذلك. فبالنسبة لمستودع البيانات هذا أو أي مستودع آخر لقاعدة بيانات إدارة التهيئة CMDB، فإنه يجب أن يكون هناك ربط قائم ومعمول به مع تلك الواجهات الأخرى.

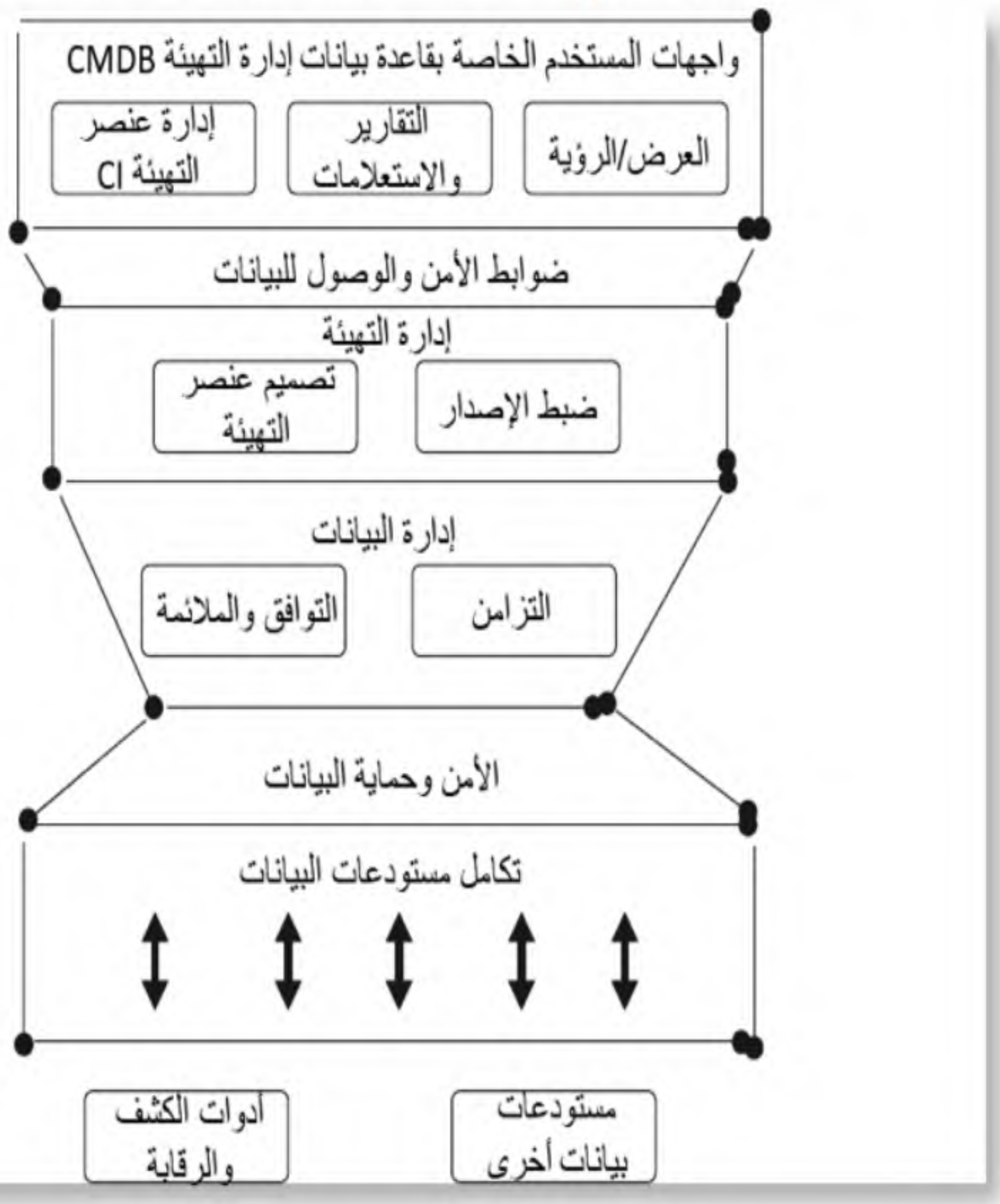
تصـف القائمة السـابقة خصائص قاعـدة بيانـات إدارة التهيئة CMDB. فبالنسـبة للمؤسسات الكبيرة والمعقدة، سيكون من الصعب إطلاق وتنفيذ مثل هذه الإدارة والعملية الخاصة بتقنية المعلومات بشكل فعال، غير أنه يجب أن تكون هناك فوائد ومنافع مستمرة مـن قدرات وكفاءات النظم. إن تطبيق قاعدة بيانـات فعالة لإدارة التهيئة CMDB يعد أحد الأدوات الهامة في كفاءة وحوكمة تقنية المعلومات بالنسبة لأي مؤسسة تمتلك مجموعة كبيرة ومعقدة نسبياً من نظم وعمليات تقنية المعلومات.

إنشاء قاعدة بيانات إدارة التهيئة CMDB في المؤسسة:

يعلـن العديد مـن باعة البرمجيات عن منتجـات خاصة بقاعدة بيانـات إدارة التهيئة CMDB عـلى أنها جزء من العروض الخاصة بهـم. وبالرغم من أن معظم هذه المنتجات يجـب أن تتفـق ومعايير إطار العمل آيتل، إلا أنه لا يوجد تعريف موحد ومتناغم بين تلك المنتجـات. وبينما يمكـن لتطبيق قاعدة بيانات إدارة التهيئـة CMDB أن يكون المشروع الرئيسي بالنسـبة للمؤسسة، فإن إدارات تقنية المعلومات الأصغر والأقل نضجاً لا ترغب في الاسـتثمار في برامج قاعدة بيانـات إدارة التهيئة CMDB المكلفة والمعقدة. حيث يمكنهم تنفيذ مجموعة محددة من عمليات إدارة التهيئة بواسطة استخدام أدوات برمجية مكتبية بسيطة مثل الإكسيل Excel. وتعد قاعدة بيانات إدارة التهيئة CMDB بمثابة نظام لإدارة المعرفـة أكـثر من كونها منتجاً من المنتجات البرمجية، كما أنها تعتبر فهرسـاً أكثر من كونها قاعدة بيانات معقدة. هذا يعني كلما كانت كمية البيانات الخاصة بعناصر التهيئة صغيرة استطاعت المؤسسة الاستفادة من مزايا قاعدة بيانات إدارة التهيئة CMDB من خلال عدة طرق - كالورق، أو مخططات VISIO، أو قواعد بيانات ACCESS، أو العقول البشرية، وما شابه. وهذا بالضبط ما تم تثبيته في العديد من المؤسسات.

شكل توضيحي (١٤-٣)

عرض تصوري لقاعدة بيانات إدارة التهيئة CMDB



من ناحية أخرى، فإنه عندما تتسع إدارة تقنية المعلومات في المؤسسة جغرافياً بشكل كبير، ويكون لديها مئات أو آلاف المستخدمين والمواقع، فإن هذا العدد المهول لتلك الاختلافات في التهيئة يتطلب حلاً من نوع خاص لقاعدة بيانات إدارة التهيئة CMDB. إن تقنية المعلومات أو الفريق الإداري الذي يبحث عن الحل المناسب أو من يقوم بتثبيته يجب أن يقوم بوضع معايير ومتطلبات خاصة بأداء نظام قاعدة بيانات إدارة التهيئة

CMDB لديهـم. لذا فان نظام قاعدة بيانات إدارة التهيئة CMDB في المؤسسـة يتطلب بعـض المزايا الفريدة. وهـي أولاً، إن الحل الحقيقي لقاعدة بيانات إدارة التهيئة CMDB يعتمد على مفهوم قديم في قاعدة البيانات يدعى نمذجة الأبعاد والذي فيه خروج بسـيط عـن النمط. وفيـه يجب أن يكون الحل الخاص بقاعدة بيانات إدارة التهيئة في المؤسسـة معتمـداً على نمـوذج قاعدة بيانات الأبعاد بـدلاً من قاعدة البيانات العلاقية الشـائعة في الوقـت الراهن. فقواعد البيانـات العلاقية الموجودة هذه الأيام مثل أوراكل Oracle ودي بي تو DB2 الخاصة بشركة IBM لا تسـتطيع القيام بالمهمـة المنوطة بقاعدة بيانات إدارة التهيئة CMDB.

وتعود هـذه المفاهيم الخاصة بنماذج قواعد البيانات العلاقيـة المقابلة لنماذج قواعد بيانات الأبعاد إلى سبعينيات القرن الماضي مع العديد من القضايا المنسية من قبل معظمنا ممن عاصروها. في هذا القسـم، سنقوم بشرح ما يحتاج إليه الحل البرمجي لقاعدة بيانات إدارة التهيئة CMDB على مسـتوى المؤسسة ومن هذه الاحتياجات: قاعدة بيانات الأبعاد واتحاد وتوافق وتزامن ونمذجة البيانات. وهنا لسنا بصدد تقديم مقالة تتحدث عن نمذجة قواعد البيانات، بل نهدف إلى إيجاز بعض المفاهيم الضرورية والرئيسـية بالنسـبة لقاعدة البيانات الفعالة لإدارة التهيئة CMDB.

معمارية قاعدة البيانات العلاقية مقابل معمارية قاعدة بيانات الأبعاد:

تسـتخدم قاعدة البيانات العلاقية أسـلوب "الصف والعمود" الذي يشبه طريقة حفظ البيانات في الجداول الإلكترونية الخاصة ببرنامج الإكسيل Excel أو في نظام معالجة المعاملات عبر الإنترنت. وسـيكون من السـهل هنا البحث عـن البيانات المخزنـة في قاعدة البيانات العلاقية في حال كنت تعرف مقدماً ما الذي تريد رؤيته. من ناحية أخرى، فإن قاعدة بيانات إدارة التهيئـة CMDB لا تقـوم بتخزين معظم بياناتها، فهي تشـير إلى بيانات محفوظة في قواعد بيانات أخرى قد تكون علاقية. وتسـتخدم قاعدة بيانات إدارة التهيئة CMDB أيضاً لتقديم ما يطلق عليه التوعية السياقية على فئات من البيانات غير المترابطة بشكل واضح.

على سبيل المثال، قد يكون الاستعلام الشائع في قاعدة بيانات إدارة التهيئة CMDB هو "ما عدد المسـتخدمين في قسـم المبيعات الذين استخدموا نظام SAP خلال الأسبوع الأخير

من الشهر؟". هذا النوع من الاستعلامات لا يتناسب بالمرة مع قاعدة بيانات علاقية مركزية من خلال معاملات اســتعلام سبق بناؤها. حيث يوجد العديد فقط من التوليفات الممكنة بين البيانات. فهذا النوع من الاستعلامات يتعين عليه سحب البيانات من عدة نظم. ومن المحتمل ألا تكون البيانات التي يحتاج إليها هذا الاستعلام مصفوفة بشكل جيد في صفوف وأعمدة جاهزة للاســتعلام. بــل يجب على قاعدة بيانــات إدارة التهيئة CMDB الخاصة بالمؤسســة أن تســتخدم تقنية الأبعاد التي تمثل البيانات كما لو كانت أبعاداً أو مستويات مختلفة.

تشــتمل أبعاد قاعدة بيانــات إدارة التهيئــة CMDB غالباً على الموقــع (مثل المدينة والولايــة والطابــق ... إلخ) ومجموعــات العمل مثل إدارة المبيعات وإدارة التســويق وما إلى ذلك، وكذلك خدمات تقنية المعلومات مثل ســاب SAP أو البريد الإلكتروني والنطاقات الزمنية وغيرها. فبدلاً من اســتخدام جداول البيانات الإلكترونية الخاصة ببرنامج الإكســيل والمكونــة من صفوف وأعمدة، ينبغــي على المرء التفكير بأحد أنــواع تمثيل البيانات الذي يدعــى مكعب روبيك Rubik's Cube ليبدأ بتكويــن الفكرة. فالمنطق المطلوب هنا ليس جديداً، فقد كان موجوداً معنا لسنوات لكن بشكل أطلقنا عليه مصطلح المعالجة التحليلية المبــاشرة المتصلــة (Online Analytical Processing (OLAP. في جميــع الأحوال، فإن التمثيل البســيط للمعالجة التحليلية المباشرة (المتصلــة) OLAP لا يعطيك قاعدة بيانات إدارة التهيئة CMDB وذلك لسببين في غاية الخصوصية: أولهما، أن معظم البيانات الخاصة بقاعدة بيانات إدارة التهيئة CMDB توجد خارج نظام قاعدة البيانات نفســها. ولكي يتم سحب البيانات من مصادر متعددة فإن ذلك يتطلب اتحاداً federation - وهو تعبيرٌ طنانٌ جديدٌ في قاعدة بيانات إدارة التهيئة (CMDB). وهو ما سنتحدث عنه في الأقسام التالية.

اتحادية قاعدة البيانات Database Federation:

إن قاعــدة بيانات إدارة التهيئة CMDB هي ما يطلــق عليها قاعدة البيانات الوصفية Metadatabase. هــذا يعني أنها عبارة عن قاعدة بيانات تشــير إلى قواعد بيانات أخرى. فالشرط الرئيسي لقاعدة بيانات إدارة التهيئة هو ما يطلق عليه نمذجة الأبعاد أو الاتحادية، وهــي عبارة عن مراجع للبيانات من مصادر متعددة. وقــد كانت القضية الخاصة بصحة

البيانات هي القضية التي أدت لأول مرة إلى اتحادية البيانات. فعندما تقوم بعمل نسـخة من شيء ما، ما هو برأيك السـند القطعي؟ الأصل أم النسـخة؟ وكيف تستطيع أن تعرف أن النسخة هي الأصل نفسه؟

إن المفاهيم التي تدور حول اتحادية قاعدة بيانات إدارة التهيئة CMDB تتعلق بكيفية الاتصال بمصادر بيانات غير متجانسة والبت بشأن أي من أجزاء البيانات تكون مؤكدة ومن ثم إنشـاء وحفظ مفاتيح لبيانات فريدة غير موجودة في أي من مصادر البيانات الخارجية إلا أنهـا لا تـزال مطلوبة. على سـبيل المثال، قد تكون البيانات غـير الموجودة في أي نظام من هذه النظم هي اسـم خدمة تقنية المعلومات ومن هم المسـتخدمون لها. كما يجب أن يكون هناك أيضاً طريقة لحفظ المعرفة (الوعي) Awareness بأنواع البيانات الموجودة في كل مصدر من مصادر البيانات التي تم توحيدها، وذلك لإجراء الاسـتعلامات الفورية أو المخصصة (غير المعرفة مسبقاً).

إن الفكـرة الخاصـة باتحادية قاعدة بيانـات إدارة التهيئـة CMDB تتطلب الاتصال بالعديـد من مصـادر البيانات، إلا أن امتلاك نظـام قاعدة بيانات إدارة التهيئة سيسـمح حقيقـة بتوحيد تلك المصادر للبيانـات. ويعد هذا أمراً في غاية الصعوبة على أرض الواقع. فالاتحـاد هو واحد فقط من متطلبات الامتثال التقنية الأربعة لقاعدة بيانات إدارة التهيئة CMDB التي لها الدرجة نفسـها من الصعوبة. لنتأمل ذلـك: ماذا لو كان هناك مخزنان من البيانات يشيران إلى البيانات نفسها؟ أي مخزن بيانات يكون قطعي الدلالة؟ ثم، الأمر الأكثر أهمية، كيف تسـتطيع أنت أن تحـدد أي منهما هو المؤكد؟ وتعد هذه من القضايا الخاصة بمطابقة وتوافقية البيانات.

توافقية البيانات في CMDB:

بـصرف النظر عـن قضية الاتصال بمصادر بيانات غير متجانسـة، والتـي من المحتمل أن تكون أيضاً تنافسـية، يمكن أن تتم بكل بسـاطة، فالمشـكلة الكبيرة التي تواجه عملية الاتحـاد الخاصة بـقاعـدة بيانات إدارة التهيئة CMDB هي ما يسـمى مطابقة البيانات Data confrontation. أثناء إنشاء المعلومات السياقية لقاعدة البيانات الوصفية الخاصة بقاعدة بيانـات إدارة التهيئة CMDB وصيانتها، يتم تحويل أجزاء أساسـية من البيانات

مــن مصادر البيانات الموحدة إلى مخــازن البيانات الخاصة بقاعدة بيانــات إدارة التهيئة CMDB. ونظــراً لأنــه من الشــائع أن يكون هناك عدة تطبيقات ونظــم متداخلة تقوم بطلب الأصول الخاصة بتقنية المعلومات نفسها أو تحتفظ بالبيانات نفسها، فمن المحتمل أن يؤدي ذلك إلى عدم تناغم البيانات وتكرارها. وهذا هو ما يعرف بمطابقة البيانات.

توافقية البيانات Data reconciliation تعني تعديل أو تكييف البيانات المســتمدة مــن أكثر من مصدر واحــد لإنهاء التكرارات والحفاظ على تناغــم البيانات. إذ لا فائدة مــن الاتحادية في ظل وجود مشــكلة التوافقية. فالتوافقية على أية حال ليســت نهاية المتطلبات بالنســبة لقاعدة بيانات إدارة التهيئة CMDB الخاصة بالمؤسسة، فما يضيف مزيداً من التعقيد لنظام قاعدة بيانات إدارة البنية CMDB هو الحاجة إلى معالجة أي تغيرات ناجمة من التسويات الصحيحة والناجحة للبيانات، وهذا ما يقودنا إلى ما يعرف بالتزامن Synchronization.

تزامن بيانات CMDB:

يمكــن أن تتغــير البيانات المخزنــة في قاعدة بيانــات إدارة التهيئــة CMDB الموحدة عند وقوع أحداث كتغيير اســم مدير المشروع (مثال "المســتخدم") أو تغيير نوع المعدات المستخدمة من Cisco series 2504 software مثلاً إلى Cisco 2801. لذا يجب أن تكون عمليــة توافقيــة البيانات قادرة على حــل هذه الاختلافات للمحافظة على ســلامة بيانات قاعدة بيانات إدارة التهيئة CMDB. لكن هذه تقنية معلومات وليســت مستودع بيانات "بسيطاً". فلا ينبغي تغيير أي عنصر من عناصر التهيئة CI الموجودة في قاعدة بيانات إدارة التهيئــة التي تتفق مع آيتل دون أن يكــون هناك طلب للتغيير. ومن ثم فإن نظام قاعدة بيانات إدارة التهيئة CMDB الذي يســتطيع أن يوحد ويعمل على توفيق البيانات بنجاح يجب عليه أيضاً أن يكون قادراً على التنبيه عندما يتم الكشــف عن تغيرات غير مصرح بها وغــير مخطط لها. فالإخفــاق في مزامنة التغيرات التي تمت تســويتها سرعان ما يؤدي إلى الخروج عن سيطرة قاعدة بيانات إدارة التهيئة CMDB، وهو ما يمكن وصفه بالكارثة.

هــذا يعني أن نظام قاعدة بيانات إدارة التهيئــة CMDB بحاجة إلى معرفة التغييرات التــي تمت الموافقــة عليها. ثم عندما يقوم محرك توافقية البيانات بكشــف وتحليل لأحد

التغيرات في البنية التحتية أو في البيانات، فعليه أن يقوم بمقارنة هذا التغيير بقائمة التغيرات المعتمــدة المتوقعــة وأن يقوم بإصدار تنبيه في حــال كان التغيير غير معتمد أن (يكون غير مخطــط له مثلاً). هــذا التنبيه يلفت انتباه مديري قاعدة بيانــات إدارة التهيئة CMDB للبيانــات الخاصــة بقاعــدة البيانات هذه. هــؤلاء المديرون بحاجة إلى مســاعدة بيانات معروضة وتصويرية ورسومية. وهو المتطلب التقني الرئيسي التالي للنمذجة.

نمذجة CMDB:

النمذجــة Modeling هــي مناظرة العلاقات المركبــة في قاعدة البيانــات ووضع تصور لهــا. وهي عبارة عن تعريفات لخدمات تقنية المعلومــات وروابط بين عناصر التهيئة CIs. فالنمذجة هي أكثر من مجرد تقرير أو عرض قوائم للموارد على شــكل أشــجار وفروع. لذا يتعــين على قاعدة بيانــات إدارة التهيئة CMDB أن تكون قادرة عــلى عرض بياناتها بصورة واضحة وبطرق تسمح للناس باستخدام تلك المعلومات لتقييم الآثار المترتبة على إدارة التغيير، وتحديــد صلاحيات إدارة مكتب الدعم الخاص بإدارة تقنية المعلومات، واكتشــاف الأعطال وإصلاحها من خلال العمليات الخاصة بإدارة الحوادث والمشاكل، والعشرات من الاستعلامات الفورية Ad hoc queries من جميع العمليات التشغيلية الخاصة بتقنية المعلومات.

إن مطلب النمذجة هذا يذهب إلى ما هو أبعد من مجرد قوائم بسيطة "لشجرة أدلة" كالتي نجدها بشــكل شــائع في بعض منتجات قاعدة بيانــات إدارة التهيئة CMDB. فلا قيمة لكل من اتحاد وتوافقية وتزامن البيانات في حال لم يتمكن المستخدمون من الحصول على إجابات نهائية ومفهومة على أســئلتهم المعقدة في أسرع وقت ممكن. ويتطلب هذا في أغلب الأحيان تمثيل العلاقات المعقدة بين عناصر البنية CIs بشكل بياني حسب الطلب.

باختصار، إن قاعدة بيانات إدارة التهيئة CMDB في المؤسســة ليست وحيدة، إنما هي عبــارة عن نظام معقد يتعين عليه توحيــد مخازن أخرى للبيانات، والتوفيق بين المنظورات البديلة أو المختلفة للبيانات نفســها، والكشــف عن التغيرات غير المصرح بها، والعمل على مزامنة التغــيرات المعتمدة مع مخازن البيانات الوصفيــة الخاصة بها وأن يكون قادر على تمثيل الهياكل (التكوينات) بيانياً وبشكل متغير حسب الطلب. وهذا ليس بالأمر السهل.

يجب على المؤسسة التي تقوم بتطوير قاعدة بيانات إدارة التهيئة CMDB الخاصة بها أن تتعهد تلك المفاهيم المتعلقة بالنمذجة المتعددة الأبعاد، وقضايا الاتحاد، والتوافقية والتزامن والنمذجة بشكل شمولي. وبالرغم من أن المدير الأول الذي يقوم بتقييم الخطط الخاصة بقاعدة بيانات إدارة التهيئة CMDB أو النظم المثبتة قد لا يكون لديه مستوى معين من الإلمام بهذه المفاهيم الخاصة بعلوم الحاسب؛ فإنه من المناسب جداً بالنسبة للمدير الأول أن يسأل أحد العاملين لديه في إدارة تقنية المعلومات عن كيفية التعامل مع هذه المسائل. وفي حال عدم ارتياحه لتلك الإجابات، فربما من الضروري العمل مع استشاري في تلك القضايا.

في جميع الأحوال، ينبغي على المؤسسة التي تعمل على إطلاق قاعدة بيانات إدارة التهيئة CMDB أن تقوم بوضع عمليات لمراقبة وضمان حدوث الاتحاد، والتوافق، والتزامن والنمذجة. فالإخفاق في إدارة تلك القضايا الحساسة والحرجة يمكن أن يحول وبشكل سريع مشروع قاعدة بيانات إدارة التهيئة CMDB من أصل Asset إلى التزام Liability.

إدارة محفظة تقنية المعلومات:

من الطبيعي أن يكون كل من إدارة تقنية المعلومات ومستخدمي تلك النظم والعمليات قد قاموا مع مرور الوقت بتنفيذ أعداد كبيرة من النظم والعمليات المرتبطة بنظم أخرى، سواء كان بشكل مباشر أم غير مباشر، أو أن تكون نظماً مستقلة وقائمة بذاتها. وفي العادة قد تم تعيين مديري تقنية المعلومات مسئولين عن بعض تلك النظم والعمليات. في حين أن الإدارات الخاصة بمستخدمي تقنية المعلومات قد يضطلعون بالمسئولية المباشرة عن النظم والعمليات الأخرى. إلا أن كل مدير مسؤول يعتقد غالباً أن النظم الخاصة به أو بها هي الأكثر أهمية عندما يكون هناك خلافات في إعداد الجداول الزمنية للأعمال أو وجود حاجة خاصة لإجراء تعديلات، أو احتياجات أخرى متعلقة بالنظم. وتتمكن إدارة تقنية المعلومات عادة من تحقيق بعض الفوائض المالية الكبيرة الخاصة بالخدمات والاستثمارات، وذلك إذا نظرت إلى تلك النظم والعمليات الخاصة بتقنية المعلومات والتي تكون غالباً متفاوتة وتقوم بإدارتها على أنها محافظ لموارد تقنية المعلومات portfolios of IT resources.

إن إدارة محفظة تقنية المعلومات تعني تقسيم وإعادة تصنيف وتطبيق إدارة الأصناف الكبيرة من موارد تقنية المعلومات. فمبادرات نظم التخطيط والمشاريع الرئيسية والجديدة في تقنية المعلومات والخدمات المستمرة لدعم تطبيقات تقنية المعلومات يمكن اعتبارها أمثلة على محافظ تقنية المعلومات.

إن الالتزام الخاص بإدارة محفظة تقنية المعلومات هو تحديد مقدار الجهود غير الرسمية لتقنية المعلومات مقدماً وتفعيل القياسات والتقييمات الموضوعية للتصورات الخاصة بالاستثمار. فمفهوم إدارة محفظة تقنية المعلومات مشابه لإدارة المحفظة المالية إلا أن هناك اختلافات كبيرة بينهما. إذ تكون أصول المحفظة المالية في العادة عبارة عن معايير ثابتة لمعلومات قياسية مثل عوائد الاستثمار. من ناحية أخرى، فإن عملية قياس قيمة تقنية المعلومات تحتاج غالباً إلى جهود كبيرة. المشكلة هي أن استثمارات تقنية المعلومات ليست متاحة كما هو الحال بالنسبة للأسهم والسندات المالية يتم غالباً قياس قيمتها باستخدام مقاييس غير مالية. هذا بالإضافة إلى أن أصول محفظة تقنية المعلومات لديها علاقة وظيفية مع المنظمة. مثل نظام إدارة المخزون الخاص بالإمدادات أو نظام الموارد البشرية الخاص بمتابعة أوضاع الموظفين. ونظراً لأهميتهم بالنسبة للمؤسسة، فمن الصعب قياسهم باعتبارها أحد أشكال محافظ تقنية المعلومات.

تقدم إدارة محفظة تقنية المعلومات مزايا وفوائد تفوق الأساليب والطرق المتبعة في الاستثمارات الخاصة بتقنية المعلومات. كما أن هناك مزايا أخرى تشمل الرقابة المركزية على الميزانية، وإدارة المخاطر، والتوافق الإستراتيجي لاستثمارات تقنية المعلومات، وطلبات استخدام النظم، وإدارة الاستثمارات إلى جانب توحيد إجراءات وقواعد وخطط الاستثمارات.

تطبيق إدارة محفظة تقنية المعلومات:

يجب على إدارة تقنية المعلومات وبالاتفاق مع المستخدمين الرئيسيين الآخرين للنظم أن يقوموا بوضع نهج إدارة المحافظ لإدارة موارد تقنية المعلومات الخاصة بها وتطوير الأهداف العامة وغايات الأداء المرجوة منها. وتختلف إدارة المحفظة عن الإدارة المالية

لتقنية المعلومات في أن لها توجهاً صريحاً وهو أن الهدف الإستراتيجي لها يرمي إلى تحديد الاستثمارات التي يجب أن نستمر فيها والاستثمارات التي يجب الانسحاب منها.

يتم تطبيق إدارة محفظة تقنية المعلومات بالنسبة للعديد من المؤسسات من خلال تقسيم موارد النظم الخاصة بها إلى ثلاثة مجالات واسعة للمحفظة مع محافظ جزئية بداخل كل مجموعة:

١- **محافظ التطبيقات:** يمكن أن تحتوي هذه المحافظ على جميع التطبيقات الإنتاجية. ويمكن أيضاً تقسيمها إلى محافظ جزئية لمجموعات مختلفة من التطبيقات مثل المالية والتطبيقات الإنتاجية الخاصة بالتصنيع وتطوير المنتجات الهندسية. الفكرة هنا هي العمل على تطابق وإدارة المحافظ التي لها المفاهيم والأهداف نفسها، كأن تكون هناك محفظة مخصصة للتطبيقات المتعلقة بالرواتب ونظم الموارد البشرية وتطبيقات تدريب الموظفين.

ويجب أن تستند محافظ التطبيقات إلى النظم القائمة مثل النظم المعتمدة على المقر الرئيسي للمؤسسة، ونظم الوحدات الميدانية والدولية والنظم الخاضعة لسيطرة المستخدم النهائي. كما يجب أن تستند جميع هذه المحافظ إلى قيمتها النسبية في المؤسسة. ويمكن أيضاً أن تستند المقارنات والتقييمات إلى مستوى المساهمة في الربحية التي تعود من استثمارات تقنية المعلومات. هذا بالإضافة إلى أنه قد تستند هذه المقارنة إلى عوامل غير ملموسة كمستوى خبرة إدارة تقنية المعلومات في تقنية محددة أو مدى إلمام مستخدميها بالتطبيقات والبنية التحتية أو قوى خارجية كظهور تقنيات جديدة وزوال أخرى قديمة.

٢- **محافظ البنية التحتية:** تركز هذه الأنواع من المحافظ على تقنية المعلومات والعمليات البرمجية الخاصة بإدارة البنية التحتية. ففي بعض الأحيان يتم تقسيم إدارة البنية التحتية إلى فئات من إدارة النظم، وإدارة الشبكة، والأمن، وبرامج إدارة التخزين. إن قدرة المؤسسات على استغلال البنية التحتية والعمليات التشغيلية وإدارة حلول التوريد والخدمات الخاصة بتقنية المعلومات لا يتوقف على إتاحة وتكلفة وفاعلية التطبيقات والخدمات فحسب، وإنما يساعد إدارة تقنية المعلومات أيضاً على الوصول إلى اتفاقات مع مقدمي الخدمات من أجل إدارة كامل عملية التوريد. وسعياً منهم

لتقليل التكاليف، وزيادة جودة تقنية المعلومات، وزيادة القدرة التنافسية للمؤسسات من خلال انتقاء مصادر وخدمات تقنية المعلومات. فإن العديد من المؤسسات وإدارات تقنيـة المعلومات التابعة لها لا ينظـرون إلى الجانب الإداري من المعادلة. ومن النتائج التـي يمكن التنبؤ بها جراء هذا الإهمال هـي المدفوعات الزائدة، وتجاوزات التكاليف، وتوقعات لم تتحقق، والفشل التام.

تسـاعد عملية إدارة محافظ نظم برمجيات البنيـة التحتية لتقنية المعلومات المختصين بالبرمجيـات على اتخاذ بعض القرارات الصعبة. على سـبيل المثال، هل نحن بالفعل نريد الترقيـة إلى إصـدار جديد لإحدى قواعد البيانات لدينـا؟ في حال كانت الإجابة نعم، كيف سـيتفاعل تطبيق قاعدة البيانات هذا مع عمليات قواعد البيانات المماثلة في جميع أنحاء المؤسسة؟ ما التكلفة الكلية التي ستتحملها المؤسسة جراء استخدام هذا المنتج؟ وما القيم التي ستحصل عليها المؤسسة منه؟

٣- **محافظ المشاريع**: ينبغي على إدارة المحافظ معالجة قضايا الإنفاق على تطوير القدرات الابتكارية من حيث العائد المحتمل من الاسـتثمار return on investment (ROI) أو الحد من تداخل الاسـتثمارات في حالات حدوث إعادة تنظيم، أو اسـتحواذ، أو الامتثال للوائـح القانونية والتنظيميـة. ويمكن الحكم على القضايا الإداريـة مع إدارة محفظة المشـاريع من خـلال معايير مثل عائد الاسـتثمار ROI والتوافق الإسـتراتيجي ونظافة البيانات وفوائض الصيانة وملاءمة الحل الناتج والقيمة النسـبية للاستثمارات الجديدة لاستبدال هذه المشاريع.

مارسـت العديد من المؤسسـات نشـاط إدارة المحافـظ على مختلف مشـاريع تقنية المعلومات والمشـاريع التشغيلية لديها من خلال تأسـيس مكاتب لإدارة المشاريع. وسيتم مناقشة عمليات إدارة المشاريع والبرامج في الفصل السادس عشر من هذا الكتاب.

مقاييس المحفظة: تحقيق القيمة من خلال إدارة محفظة تقنية المعلومات:

لن يكـون لعملية تقسـيم تطبيقات تقنيـة المعلومات والمصادر الأخـرى إلى محافظ منفصلة قيمة كبيرة بالنسـبة للمؤسسة ما لم يتم وضع بعض المقاييس لتقييم قيم المحافظ

والمســاعدة في اتخاذ قرارات أخرى متعلقة بمحافظ تقنيــة المعلومات. يجب أن نتذكر أن محفظــة تقنية المعلومات هي عبارة عن مجموعة من المبادرات والمشــاريع و/ أو البرامج التي تحقق فوائد وتأثيرات واسعة المدى.

وعــلى الرغــم من أن لدينــا مجموعة متنوعة مــن محافظ تقنية المعلومــات التي تم إنشاؤها، فإنه ينبغي على المجموعات الإدارية المناسبة وضع مهمة سارية لكل محفظة من هذه المحافظ المتنوعة لتقنية المعلومات. قد يكون للمرء هدف نحو تعزيز نمو الأعمال في مجالات محددة تمت تغطيتها بواســطة مجموعة من التطبيقات بواسطة عدة مليارات من الدولارات، في حين قد يسعى شخص آخر إلى تحقيق زيادة ملحوظة في مستوى رضا العميل، وآخر قد يسعى إلى زيادة إيرادات المؤسسة من خلال تطوير منتجات جديدة.

الخطوة التالية هي بناء إســتراتيجيات لتحقيق كل هدف من أهداف المحافظ ومن ثم وضــع مقاييــس لقياس مدى نجاحها. وتقتضي النظرة الشــمولية هنا أن ننظر إلى مختلف تطبيقات وموارد تقنية المعلومات من حيث حجم مســاهمتها في تحقيق القيمة المكتسبة مــن جميع العمليات التشــغيلية الخاصة بالمؤسســة. وبالطبع عندما تفشــل المحفظة في تحقيق رسالتها وأهدافها المرجوة، فقد يكون هذا هو الوقت المناسب لإجراء بعض التغيرات وربما يشــتمل هذا على إعادة تشكيل مكونات المحفظة، أو تغيير الأساليب بشكل كامل أو جلب أشخاص آخرين والزج بهم في هذا الخليط.

يتعــين على عمليات إدارة محفظة تقنية المعلومات وكذلك النظم القوية لإدارة التهيئة، أن تُحسِّــن الأداء الشامل لـتقنية المعلومات وتُحسِّــن كذلك العمليات التشغيلية لحوكمة تقنيــة المعلومات. كــما يجب على كل من هذين المجالين تشــجيع كل من موظفي تقنية المعلومات والإدارة العامة على التفكير بشكل أفضل بالعمليات التشغيلية لتقنية المعلومات كما لو كانت مشاريع استثمارية لأعمال المؤسسة.

الفصل الخامس عشر
عمليات تنفيذ النظم التطبيقية وحوكمة تقنية المعلومات

كانــت عملية تطويــر النظم التطبيقية في فــترة من الفترات مصدر قلق كبير بالنســبة لإدارات تقنيــة المعلومات. وذلك عندما كانــت معظم وحدات برمجة وتطوير نظم تقنية المعلومات تقوم بتصميم النظم الجديدة الخاصة بها وتكتب البرامج باستخدام موارد قسم تقنيــة المعلومات وتقوم بتنفيذ واختبار المكونات البرمجية الأساســية للتطبيقات الجديدة. وقــد كانت عمليــة التطوير هذه في بعض الأحيان تقود بعض المؤسســات إلى نفق مظلم. وكان يتــم عادة تســليم تطبيقات تقنية المعلومات الجديدة المحليــة أو المطورة داخلياً في وقت متأخر أي بعد الوقت المحدد بكثير، وكان يتم اختبار تلك الأنظمة بشكل ضعيف، ولم تكن تحقق أهدافها المعلنة. والأسوأ من ذلك، أنه كان في بعض الأحيان يتم إطلاق مشاريع تطبيقات جديدة دون فهم واضح لأهداف النظام. ويعود هذا العصر من مشــاريع تطوير التطبيقات الفاشلة إلى الأيام الأولى لظهور تقنية المعلومات. وذلك عندما شعر الجميع بأن متطلبــات نظم تقنية المعلومات الخاصة بهم عبارة عن متطلبات فريدة من نوعها وخاصة بأنظمتهم فقط. الأمر الذي اســتوجب عليهم القيام بتطوير التطبيقات الخاصة بهم لدعم وتحقيق تلك المتطلبات الفريدة والخاصة بهم.

وفي الوقت الذي كان مؤلف هذا الكتاب يســترجع تاريخه ليبين ذلك، فقد أقر بأنه كان يعمــل ذات يوم في إحدى شركات تقنية المعلومات حيث كانت هناك جهود خاصة بتطوير النظــم من أجل تطوير تطبيقات جديدة خاصة بحســابات المدفوعــات - وقد كان آنذاك عبارة عن تطبيق لتحرير الشــيكات بصورة فعالــة – أو حتى لتطوير وبرمجة نظم جديدة لمعالجــة الرواتب! وذلك في ضــوء القوانين الخاصة بالولاية أو القوانــين الوطنية، فقد كان هناك بالفعــل اختلافات ضئيلة بين المتطلبات الخاصة بأحد نظم الرواتب مقابل متطلبات غــيره من النظــم. من جهة أخرى، وبالعودة إلى تلك الأيام فقــد كان هناك عدد قليل من التطبيقات التي يتم تطويرها بشــكل تجاري لاســتئجارها أو شرائها. أما اليوم، فإننا بشكل عــام نقوم بــشراء هذا النوع من البرمجيــات من أحد الموردين الخارجيــين الذين يقومون

بتوريد البرمجيات والتحديثات الخاصة بها على نظام حاسبات الخادم - العميل الموجود في مكاتب المؤسسة أو إتاحة تلك البرمجيات من خلال بيئة الحوسبة السحابية (انظر الفصل التاسع من هذا الكتاب الذي يتحدث عن الحوسبة السحابية).

وعلى الرغم من الانتقال هذه الأيام من التطبيقات المطورة داخلياً إلى التركيز أكثر على البرمجيات التي يتم شراؤها وتوريدها من قبل أحد الباعة؛ لا تزال هناك حاجة لدى المؤسسة بأن تقوم بتطوير وبناء واختبار بعض نظم التطبيقات الخاصة بها أو أن تقوم بالتعديل على بعض التطبيقات التي قامت بشرائها. ويعد هذا الأمر واقعياً على وجه الخصوص عندما تقوم المؤسسة بتطبيق أحد نظم قواعد البيانات المعقدة ذات المهام المتعددة والمترابطة والمعروفة بنظم تخطيط موارد المؤسسة إي آر بي (Enterprise Resource Planning (ERP. حيث تمتلك هذه النظم المعقدة التي يتم توفيرها من قبل الباعة القدرة على ربط جميع وظائف التطبيقات تقريباً في مجموعة واحدة من قواعد البيانات المترابطة. على سبيل المثال، عند تثبيت نظام ERP في بيئة نظام صناعي، فإن تنفيذ طلب شراء منتج قد يتسبب في إحداث تغيرات في كل من نظام التصنيع ونظام الإنتاج، حيث يتم وضع أمر التوريد عند الحاجة إلى مواد اضافية وغيرها من العمليات الكاملة لبيع وشحن الانتاج.

وكعنصر أساسي من عناصر العمليات الرشيدة لحوكمة تقنية المعلومات، فإن المؤسسة تحتاج إلى عمليات قوية لتطوير نظم تقنية المعلومات، سواء لبناء تطبيقات بطرق تقليدية أم للحصول على ترخيص من البائع فيما يخص التطبيق السحابي.

يناقش هذا الفصل الجوانب الخاصة بحوكمة تقنية المعلومات فيما يتعلق بأساليب تطوير التطبيقات الخاصة بتقنية المعلومات من منظور التطبيقات التي تم تطويرها عبر عمليات تطوير نظم معتمدة ومعروفة جيداً، مروراً بالعمليات الشائعة لتطوير التطبيقات السريعة باستخدام تطبيقات لإنشاء أنواع مختلفة من التقارير، ووصولاً إلى قواعد البيانات الشاملة لنظام تخطيط موارد المؤسسة ERP. لذا يجب أن يكون لدى إدارة المؤسسة فهم جيد لعمليات حوكمة تقنية المعلومات التي تحيط بجهودها المبذولة لتطوير تطبيقات نظم جديدة.

دورة حياة تطوير النظم: إحدى التقنيات الأساسية لتطوير التطبيقات:

لقد كانت السـنوات الأولى لتطوير تطبيقات تقنيـة المعلومات مليئة بالكوارث فيما يخص النظم الجديدة في العديد من المؤسسـات. كان المدير الأول - غالباً المراقب المالي للمنظمة - يقوم بإخبار رئيس قسـم تقنية المعلومات بأنه يريد تطبيقاً جديداً لتحقيق حاجة ما. وبدون إجـراء المزيـد من عمليـات التحليل يقوم فريق البرمجـة بالتجمع لكتابة برامـج لتلبية هذه الحاجـة. وكانت النتائج فاشـلة غالباً. حتى وإن كانت تلك التطبيقـات الجديدة تعمل وتم تسليمها في الموعد المناسب، فإنها لم تكن تلبي غالباً متطلبات وتوقعات الإدارة. إننا نتكلم هنا عن الأيام الأولى لنظم الحاسـبات المركزية mainframe لـتقنية المعلومات عندما كانت عملية شراء البرمجيات غير معروفة وكان الجميع يقومون بإنتاج التطبيقات الخاصة بهم.

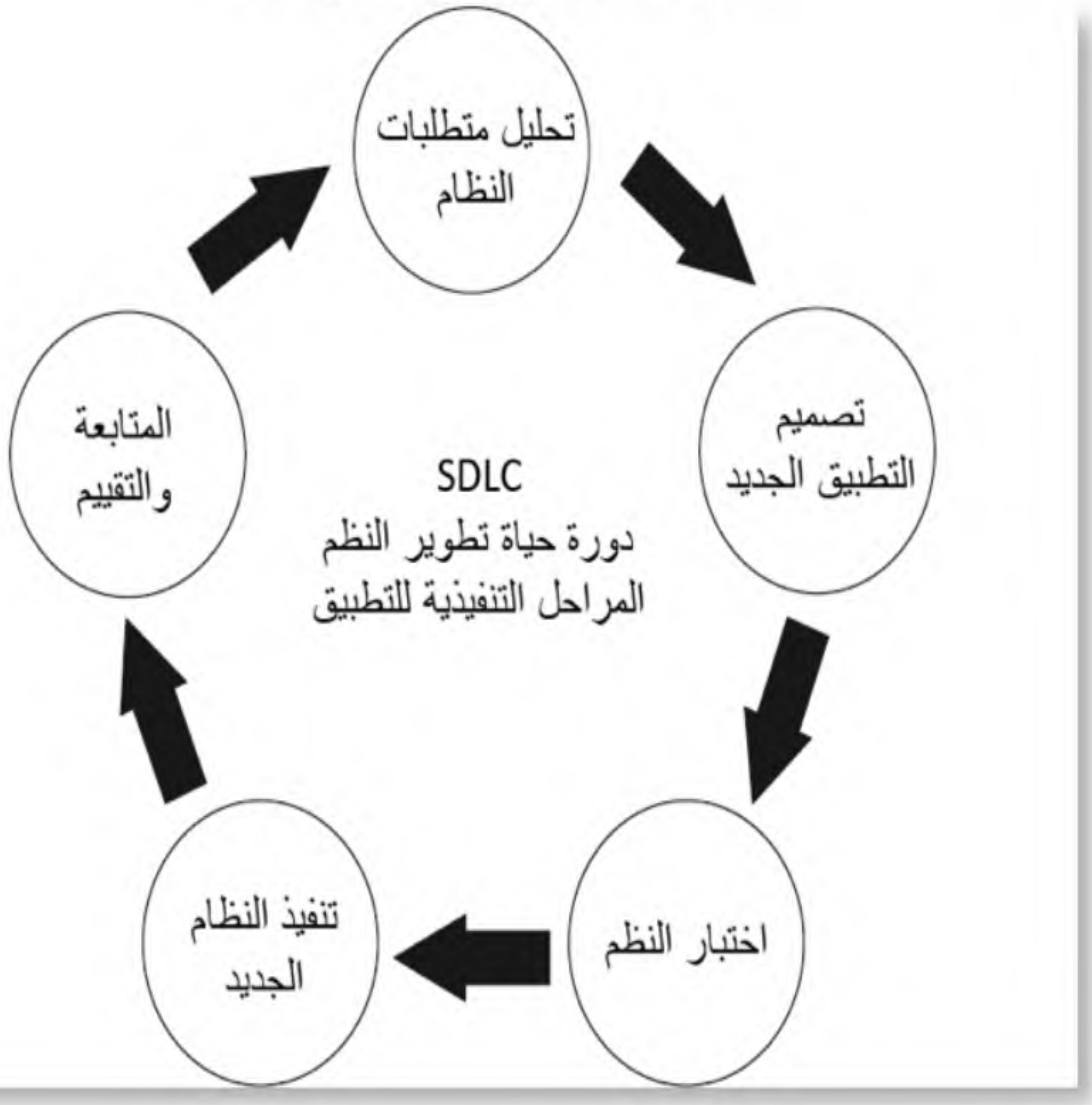
بالتأكيـد لم تكن المفاهيم الخاصـة بـحوكمة تقنية المعلومـات معروفة في تلك الأيام المبكـرة التي كانت تتميز بوجود نظم الحاسـبات المركزية، وبرامـج الكوبول COBOL، والتـي كانـت تتميز بوجه خاص بوجود النظـم الموجهة نحو الدفعـة batch-oriented systems، وقـد كان هنـاك بالتأكيد العديد من الإخفاقات الخاصـة بـتطوير التطبيقات. ولتنظيـم عملية تطوير النظـم وقتها، قامت شركة IBM وهي المـزود الرئيسي للمعدات والبرمجيات في تلك الأيام بإطلاق نهج خاص بتطوير النظم عُرِفَ بدورة حياة تطوير النظم Systems Development Life Cycle (SDLC). وعـلى الرغـم من محاولة العديد من الشركات الأخرى إنتاج أساليب أخرى مختلفة لتطوير النظم، فإن نهج SDLC أصبح بمثابة العملية الرئيسية لتطوير التطبيقات الفعالة في تقنية المعلومات.

يعرض الشـكل التوضيحي (١٥-١) الخطوات العملية الأساسـية لنهج SDLC في شكل عملية دائرية أو مسـتمرة. ومع أن المؤسسة وإدارة تقنية المعلومات التابعة لها بإمكانهم البـدء بعملية تطوير النظم من أي نقطة، فـإن هناك أولاً حاجة لعملية تحليل المتطلبات، وهـذا يعني أنه قبل أن تبدأ وحدة تقنية المعلومات بأي عمل يتعلق بتطوير النظم، يجب عليها أولاً الحصول على تفاهم رسـمي حول الأهـداف والتوقعات الخاصة بمشروع النظام الجديد. ومن الطبيعي أن يتم التوثيق والتصديق على ما تم الاتفاق عليه من خلال عملية إدارية مع عمل تقديرات أولية لتكاليف النظام الجديد والفوائد المتوقعة منه.

وبمجــرد أن تتم الموافقة على التطبيق الجديد، يتعين الانتقال إلى مرحلة أخرى رســمية مــن تصميم وبرمجة التطبيق. ويجب أن يتم تطوير وتوثيق كل برنامج ومكون من برامج ومكونــات النظام الجديد ومن ثم اختباره باعتبارها وحدة مســتقلة. ثم ننتقل بعدها إلى مرحلة اختبار وتطبيق النظم بالكامل، الأمر الذي يؤدي إلى تطبيق النظام.

شكل توضيحي (١٥-١)

مراحل دورة حياة تطوير النظم SDL



إن المفهوم الشامل من وراء عملية دورة حياة تطوير النظم SDLC هي أنه عند تنفيذ تطبيق جديد، ينبغي على إدارة تقنية المعلومات وإدارة المؤسسة مراقبة نجاح وتقدم هذا التطبيق الجديد. الأمر الذي قد يؤدي إلى الحاجة إلى إجراء تعديلات أو تنقيحات على النظام أو الحاجة إلى نظام جديد كلياً. ومن ثم فإن دورة حياة تطوير النظم SDLC هي عملية تحسين مستمرة تهدف إلى تطوير التطبيقات الجديدة الخاصة بتقنية المعلومات ومراقبتها بشكل مستمر. وتعود عملية دورة حياة تطوير النظم SDLC تاريخياً إلى زمن نظم الحواسيب المركزية ونظم الدفعة التي كانت وقتها تحتاج إلى موافقات ووثائق تفصيلية كثيرة لكل خطوة من خطوات العملية.

وعلى الرغم من تحولنا الآن إلى التطوير السريع وعمليات تطوير تطبيقات النماذج التي تعتمد بشكل كبير على البرمجيات التي يوفرها البائع، فإن العناصر الرئيسية لعملية دورة حياة تطوير النظم SDLC يجب أن تبقى في موضع التنفيذ بالنسبة لأي عملية تطوير لتطبيقات جديدة في تقنية المعلومات. هذا يعني أن تطبيقات النظم الجديدة يجب أن تسير دائماً من خلال عملية رسمية لتحليل متطلبات النظم وعمليات رسمية لإطلاق التطبيقات وعمليات لتحسين تلك التطبيقات والاستغناء عنها في أواخر حياتها.

بالاعتماد على نوع وطبيعة عملية تطوير نظم تطبيقات تقنية المعلومات، فإن عملية تحليل المتطلبات يمكن أن تكون غير رسمية أو رسمية للغاية. إلا أن الشكل التوضيحي (١٥-٢) يوجز لنا محتويات العملية التقليدية لتحليل متطلبات تطوير النظم. إن المفتاح الرئيسي لهذه العملية هو أنه يجب على فريق المشروع أن يلقي نظرة فاحصة على طلبات المستخدمين وحتى على طلبات إدارة تقنية المعلومات المتعلقة بالتطبيق الجديد وتحديد ما إذا كانت هذه الطلبات منطقية أم لا. ما يحدث في الواقع، هو أن العديد من الطلبات الخاصة بتطبيق تقنية المعلومات يتم استبعادها بعد التحليل الأوّليّ للنظم. وعلى أي حال، فإن عملية تحليل المتطلبات توفر آلية رسمية لمراجعة الطلبات الجديدة الخاصة بالتطبيق الجديد وتحديد ما إذا كانت هذه الطلبات منطقية أم لا.

يعد تحليل المتطلبات خطوة واحدة فقط من الخطوات الموجودة في دورة حياة تطوير النظم، إلا أنه يجب تضمينها دائماً في عملية تطوير النظم. وكأحد المكونات الرئيسية في عملية

حوكمـة تقنية المعلومات، فإنه ينبغي على المؤسسـة وإدارة تقنيـة المعلومات التابعة لها أن تمتلك نموذجاً من النماذج المعمول بها لعملية دورة حياة تطوير النظم SDLC، حتى في حال استخدامهم لعمليات التطوير السريع، كالنمذجة التي سنتحدث عنها في الفقرات التالية.

عمليات التطوير السريع في تقنية المعلومات: النمذجة (Prototyping):

إن استخدام العمليات الرسمية لدورة حياة تطوير النظم SDLC كان له أثر ومعنى كبير في الأيام الأولى لنظم تقنية المعلومات، وذلك عندما كانت المؤسسات هي التي تقوم بتطوير وبرمجة تطبيقاتها بشـكل كامل، وعندما كان هنـاك حاجة لتوثيق وصياغة عمليات تطوير النظم الجديدة بشـكل رسـمي. وقد كان، هناك مجموعة متنوعة من التجار الذين قاموا ببيع أساليب تطوير الأعمال وإدارات تقنية المعلومات التابعة لها. وقد كانت المنتجات التي يتم تسـويقها في ذلك الوقت تطلب من مطوري النظـم أن يقوموا بتحضير وثائق تفصيلية عـن جميع مراحل الأعمال التي قاموا بإنجازها. وباتباع ذلك بالشـكل السـليم، أدت تلك المنهجيـات إلى الوصـول لنظم تطبيقـات جديدة موثقة ومخطط لها عـلى نحو جيد. كان هدفها هو مجرد تحسـين عملية تطوير وتنفيذ التطبيقات الجديدة لتقنية المعلومات. وقد كانت المشكلة الوحيدة وقتها أن المنهجيات الكثيرة الخاصة بتطوير الوثائق كانت في كثير من الأحيان لا تعمل بشكل جيد. فقد كانت المنهجيات المنشورة وقتها تتطلب استكمال العديد من الوثائق الرسـمية، وجميعها يحتاج إلى مراجعات وموافقات. ومع ذلك، فقد قامت كل من وحدة تقنية المعلومات والإدارة بالنظر في أعمال التطوير الجديدة وكانت باستمرار تقرر أموراً ليست صحيحة تماماً وتبحث باستمرار عن تغيرات وتنقيحات تكون ثانوية غالباً.

لم يعد هناك وجود بالأسـاس لبائعي هذه المنهجيات الرسـمية المنشـورة لدورة حياة تطويـر النظم SDLC، تماماً كـما ابتعدنا نحن عن النظم الرسـمية للحاسـبات المركزية Mainframe. أما اليوم فهناك تطبيقات جديدة يتم بناؤها غالباً من خلال أدوات برمجية سهلة الاستخدام تعتمد على الجداول. حيث إننا نقوم ببناء إصدار أوليّ أو نموذجي، ومن ثـم نقوم بتعديل هذا النمـوذج ليتوافق مع المتطلبات، ثم نقـوم بتنفيذ التطبيق. هذه الأنـواع من التطبيقات تم تطويرها من خلال عملية تسـمى التطوير السريع للتطبيقات Rapid Application Development (RAD). وهي منهجية لتطوير البرمجيات تعتمد

علـى اسـتخدام الحد الأدنى من أسـاليب التخطيط والنماذج المبدئية لإطلاق النسـخة أو الإصدار الأوّلي، ومن ثم يتم ضبطه وتعديله حتى ينال استحسان الجميع. وينظر كل من المسـتخدمين ووحدة تقنية المعلومات إلى هذا الإصـدار للنموذج المبدئي ويقومون بإجراء المزيـد من التغيـيرات ليصلوا في نهاية المطـاف إلى التطبيق النهـائي. إن هذا القصور في التخطيط المسـبق المكثف بشكل عام يسمح بكتابة البرمجيات بشكل أسرع بكثير ويجعل عملية تغيير المتطلبات أكثر سـهولة. يوضح الشـكل التوضيحي (١٥-٣) نسـخة مبسطة لعملية تطوير البرمجيات القائمة على منهجية التطوير السريع RAD.

شكل توضيحي (١٥-٢)

عملية تحليل المتطلبات الخاصة بتطوير النظم.

• **التحضير لتحليل متطلبات النظم:** تعيين أعضاء فريق المشروع وجمع المعلومات الأساسية، متضمناً ذلـك المجموعات التي قامت بوضع وتحديد هذه المتطلبات وغيرهم من مجموعات المسـتخدمين المحتمل مشاركتهم في هذه العملية للسماح بجمع وتحليل متطلبات النظام.
• **تحديد متطلبات الأعمال:** تحديد كل المتطلبات سواء كانت داخل النطاق أم خارج النطاق، وتحديد وتوثيق قواعد الأعمال المخطط لها، بالإضافة إلى تحديد الواجهات المحتملة من وإلى التطبيق الجديد.
• **تحديد نموذج العمليات.** تحديد وتخطيط العمليات الرئيسـية للأعمال التي ستتعامل مع التطبيق الجديد المقترح. ثم تجزئة هذه العمليات إلى وظائف رئيسية وفرعية يمكن التحكم بها حتى نصل إلى حد لا يمكن فيه تقسيمها أكثر من ذلك.
• **تحديد نموذج بيانات منطقي:** فهم ونمذجة البيانات بشكل منطقي لدعم التطبيق المقترح. وتحديد كيانـات التطبيق وعلاقاتها بالكيانـات الأخرى، هذا بالإضافة إلى تحديد السـمات أو الحقول التي تتوافق مع الأعمال.
• **تحقيـق التوافـق بين متطلبات الأعمال والنمـوذج:** يجب على فريق المـشروع التأكد من أن كلاً من العملية التي تم تعريفها والنموذج المنطقي للبيانات يستوعب جميع المتطلبات وقواعد العمل.
• **وضـع المواصفـات الوظيفية:** لا بد من دمـج الواجهات الأمامية والعمليـات والبيانات لكي تصف بشـكل نظامي كيف يمكن للمسـتخدم المحتمل أن يستخدم النظام وكيف يمكن استرجاع ومعالجة وتخزين البيانات المرتبطة.

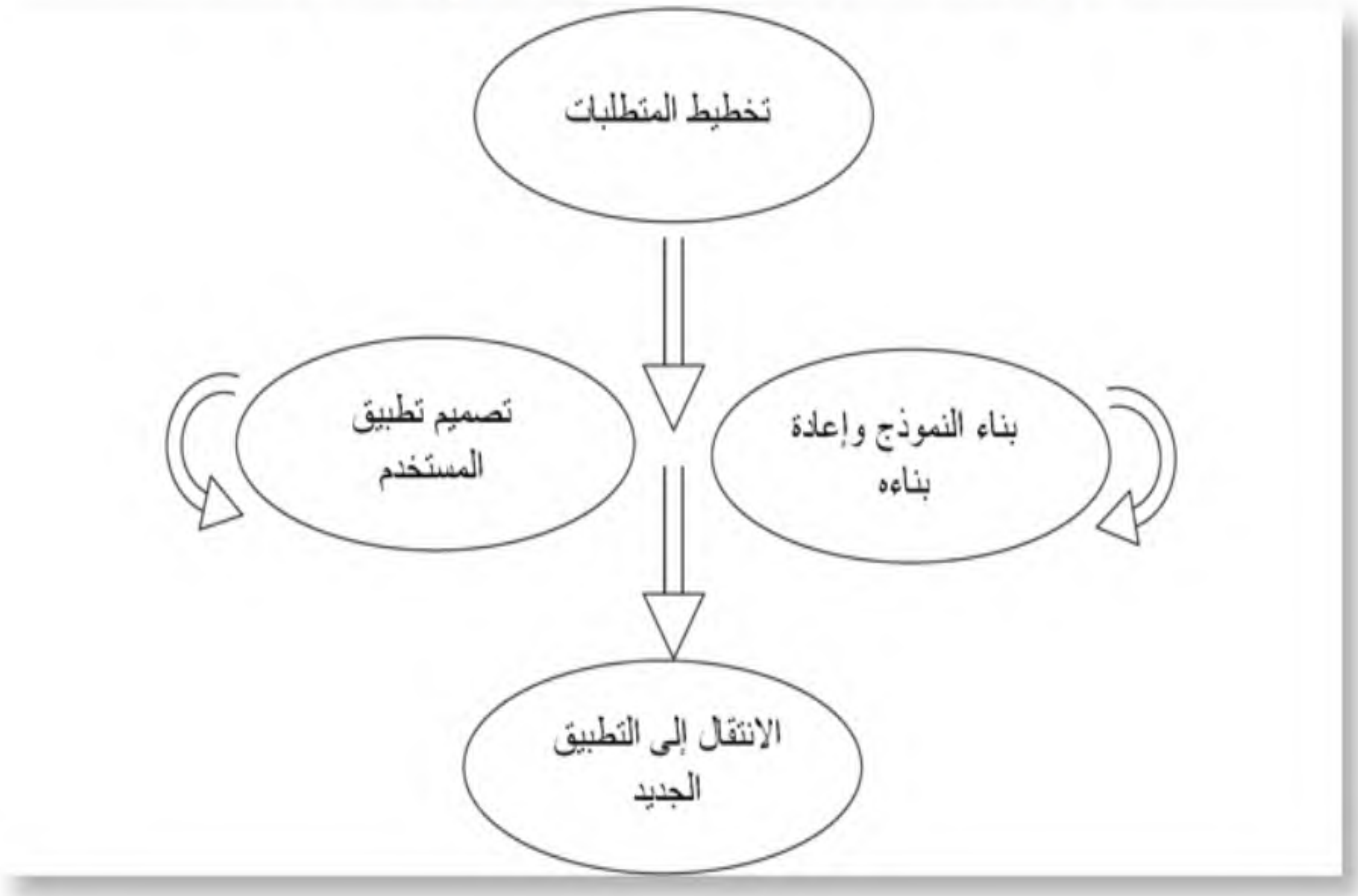
تبدأ عملية التطوير السريع للتطبيقات RAD بتطوير النماذج الأولية للبيانات وعمليات الأعمال لتتمكن من تحديد المتطلبات الأولية. ويمكن إصدار عينة أو نموذج مبدئي من التطبيق باستخدام واحدة من الأدوات البرمجية القوية المتخصصة بإنشاء التقارير هذه الأيام. ومن ثم يتم فحص هذا النموذج مقابل المتطلبات الموجودة حتى يتسنى إدخال التحسينات اللازمة على نماذج البيانات والعمليات. هذه المراحل تتكرر بشكل دوري؛ فهناك مزيد من مخرجات التطوير موجودة في بيان شامل يجمع متطلبات الأعمال والتصميم التقني ليتم استخدامها في بناء نظم جديدة.

يترتب غالباً على أساليب التطوير السريع للتطبيقات RAD تقديم تنازلات على مستوى الأداء الوظيفي وأداء التطبيق بشكل عام في مقابل تمكين تطوير أسرع وتسهيل صيانة التطبيق. تتكون عملية التطوير السريع للنظم من المراحل الأربع التالية:

١- **مرحلة تخطيط المتطلبات في RAD:** يجب على تقنية المعلومات في المؤسسة أن تستخدم بعض العناصر نفسها الموجودة في مراحل تخطيط وتحليل النظم للعملية التقليدية الخاصة بدورة حياة تطوير النظم SDLC الموضحة في الشكل التوضيحي (١٥-٢). في جميع الأحوال، ووفقاً لأسلوب التطوير السريع للتطبيقات فإنه يتعين على المستخدمين، والمديرين، وأعضاء فريق تقنية المعلومات، مناقشة متطلبات الأعمال، ونطاق المشروع، والقيود، ومتطلبات النظام والموافقة عليها. تنتهي هذه المرحلة عندما يتفق الفريق على القضايا الرئيسية والحصول على تصريح من الإدارة بالاستمرار.

شكل توضيحي (١٥-٣)

عملية تطوير البرمجيات وفقاً لأسلوب التطوير السريع للتطبيقات RAD



٢- **مرحلة تصميم تطبيقات المســتخدم في RAD:** في هذه المرحلة يعمل المستخدمون مع محللــي النظم على وضع النماذج والنــماذج الأولية التي تمثل جميع عمليات ومدخلات ومخرجات النظم. وتقوم عادة المجموعات الرئيسية والفرعية المشاركة في عملية التطوير السريع للتطبيقات RAD باســتخدام أدوات تطوير التطبيقات الموجودة في إدارة تقنية المعلومات لترجمة احتياجات المستخدم إلى نماذج عمل. وتعد مرحلة تصميم تطبيقات المستخدم عملية تفاعلية مستمرة فهي تسمح للمستخدمين بفهم وتعديل نموذج العمل الخاص بالنظام الذي يلبي جميع احتياجاتهم.

٣- **مرحلة البناء:** تركز هذه المرحلة على مهام تطوير برامج وتطبيقات مشابهة لعملية دورة حيــاة تطوير النظم SDLC. وطبقــاً لنهج التطوير السريع للتطبيقات، فإنه ومن ناحية

أخرى، يستمر المستخدمون في المشاركة واقتراح التعديلات والتحسينات عند التطوير الفعلي للشاشات والتقارير. وتتمثل مهام هذه المرحلة في البرمجة وتطوير التطبيقات، وكتابة التعليمات البرمجية، وتكامل الوحدات واختبار النظام.

٤- **مرحلة الانتقال في RAD:** تشبه هذه المرحلة الأخيرة المهام الأخيرة الموجودة في تطبيق دورة حياة تطوير النظم SDLC بما فيها تحويل البيانات والاختبار والتحول إلى النظام الجديد وتدريب المستخدمين. وبالمقارنة مع الطرق التقليدية، فإنه يتم ضغط العملية برمتها. ونتيجة لذلك، فإنه يتم بناء النظام الجديد وتسليمه ووضعه موضع التشغيل بشكل أسرع بكثير. فمهام هذه المرحلة هي تحويل البيانات واختبار النظام بأكمله وتحويل النظام وتدريب المستخدمين.

لقد بدأ نهج التطوير السريع للنظم RAD الخاص بتطوير النظم في الوقت الذي بدأت فيه المؤسسات وإدارات تقنية المعلومات التابعة لها في الانتقال من نظم الحاسبات المركزية القديمة إلى نظم العميل-الخادم، وذلك أثناء زيادة هيمنة نظم الحاسبات المحمولة والحاسبات المكتبية، والأكثر أهمية من ذلك هو ظهور الإنترنت. وبالعودة إلى أيام دورة حياة تطوير نظم SDLC الخاصة بالحاسبات الكبيرة المركزية، فقد عبر العديد من مستخدمي تقنية المعلومات داخل المؤسسة وقتها عن استيائهم من عمليات التطوير البطيئة وفشل النظم الجديدة والميزانيات المهدرة ومجموعة من المشاكل الأخرى. إن تقديم أدوات التطوير السريع للتطبيقات RAD إلى مستخدمي النظم هؤلاء كان أشبه بالتجلي. فقد تمكنوا من إلقاء نظرة سريعة على إصدارات النماذج الأولية لتقارير وحتى عمليات النظم ومن ثم استطاعوا المضي قدماً من خلال الإصدار السريع والفعال لنهج التطوير السريع للتطبيقات RAD.

ونظراً لسهولة استخدامها، فإن المؤسسات التي تشجع على استخدام أدوات التطوير السريع للتطبيقات RAD قد تجد نفسها في مشاكل تتعلق بالأمن والضوابط الداخلية للتطبيقات في حال استخدمت نهج التطوير السريع للتطبيقات RAD بشراسة لتطوير التطبيقات الجديدة دون وضع الضوابط الملائمة على التطبيقات

الجديدة. الشكل التوضيحي (١٥-٤) يوجز لنا بعض ضوابط وإجراءات حوكمة تقنية المعلومات التي لا بد من وجودها في المحيط الذي تُستخدم فيه عمليات التطوير السريع للتطبيقات RAD.

تقوم العديد من المؤسسات هذه الأيام بتطوير تقاريرها الخاصة بها والتي يتم إنشاؤها حسب الطلب لدعم تطبيقات البرمجيات التي تم شراؤها. ويتم اليوم تطوير تطبيقات البرمجيات التي يتم شراؤها بصورة شبه دائمة باستخدام أداة خاصة لإنشاء التقارير أو باستخدام إحدى أدوات التطوير السريع للتطبيقات الخاصة بهذه البرمجية. ويمكن تطبيق أفضل ممارسات حوكمة تقنية المعلومات التي تمت مناقشتها في هذا الفصل على جميع هذه الأدوات.

تخطيط موارد المؤسسة وعمليات حوكمة تقنية المعلومات:

يتم عادة توظيف أحد قواعد البيانات الشاملة للعمل على أنه مستودع للبيانات، حيث تعمل نظم تخطيط موارد المؤسسة (ERP) على تكامل المعلومات الإدارية الداخلية والخارجية عبر المؤسسة بالكامل حيث تشتمل على نظم الإدارة المالية، وإدارة التصنيع عند الحاجة، وإدارة المبيعات والخدمات وإدارة علاقات العملاء وغير ذلك. وتعد نظم ERP من قواعد البيانات المعقدة التي تعمل على أتمته هذا النشاط من خلال تطبيقات البرمجيات المتكاملة. حيث إن الغرض من هذه النظم هو تسهيل تدفق المعلومات بين جميع وحدات الأعمال داخل حدود المنظمة وإدارة الاتصالات مع أصحاب المصالح الخارجيين. إذاً فالهدف من نظام ERP هو تحسين وتبسيط العمليات الداخلية للأعمال، والذي يتطلب عادةً إعادة هندسة العمليات الحالية لتلك الأعمال.

شكل توضيحي (١٥-٤)

ضوابط وإجراءات حوكمة تقنية المعلومات المتعلقة بالتطوير السريع للتطبيقات RAD.

إن التطويــر السريع للتطبيقات RAD هو أســلوب لتطوير البرمجيــات. حيث يركز على فترات زمنيــة قصــيرة للتطوير (من ٣٠ إلى ٩٠ يوماً). وهذا الأســلوب لا يصلح في تطوير التطبيقات المعقدة أو التطبيقــات التــي تعالج كميات كبيرة من المعاملات بشــكل سريع مثل البيئــات الخاصة بمعالجة الدفعة. وقد يكون من المناسب بالنسبة للمؤسسة أن تستخدم هذا الأسلوب لتطوير أو إعادة تصميم التطبيقــات ذات المخاطر المنخفضــة أو التطبيقات الأقل تعقيداً مثل مواقــع الويب (الإنترنت) ذات المعاملات التي لا تحتوي على طاقة إنتاجية عالية المســتوى Throughput. إضافة إلى ذلك، واستناداً إلى درجــة تحمل المؤسســة للمخاطر وتحديد المهام الحساســة والحرجة للتطبيــق، فإنه يتحتم على المؤسسة اســتخدام الضوابط والإجراءات الخاصة بحوكمة تقنية المعلومات لضمان توظيف الأساليب المناســبة الخاصة بالتطوير السريع للتطبيقات RAD أثناء مراحل التصميم والتطوير للتطبيق الجديد في تقنيــة المعلومات ضمن منهجيــة تطوير مهيكلة. والنقاط التالية توجز بعض الضوابط والإجراءات العامة والجيدة في حوكمة تقنية المعلومات:
• اختر أداة مناســبة لتوليد تقارير التطبيقــات بحيث تكون مرنة وتلبي احتياجات تطبيقات الأعمال. كما يتعين على الإدارة ضمان أن أســلوب التطوير الذي تم اختياره مناســب لإدارة تعقيدية ومخاطر التطبيقات التي بصدد تطويرها.
• ضع قواعد لتقنية المعلومات مثل أنه سيتم فقط استخدام تقنية التطوير السريع للتطبيقات RAD التــي تمت الموافقة عليها لأغراض التطبيقات الإنتاجية مــا لم تكن هناك موافقة محددة من الإدارة العليا لتقنية المعلومات.
• نفذ برامج تدريبية أولية ومســتمرة لكادر تقنية المعلومات والمستخدمين المعنيين تتعلق باستخدام الأداة البرمجية التي تم اختيارها للتطوير السريع لتطبيقات RAD.
• ضــع معايير خاصة بإدارة تقنية المعلومات فيــما يتعلق بالتطبيقات المطورة خلال عمليات التطوير السريــع للتطبيقات RAD والتي تضم المراحل الرســمية للبدء، والتطويــر، والتنفيذ. حيث تتطلب الفترة الزمنية القصيرة لمشاريع التطوير السريع للتطبيقات RAD ضرورة الإسراع في تحديد المتطلبات الوظيفية التي يجب أن تبقى إلى حد كبير دون تغيير أثناء عملية التطوير.

• حدِّد أي المســتويات المناســبة من العاملين والمســتخدمين النهائيين في تقنية المعلومات هم الذين ســيتم تعيينهم في مشــاريع التطوير السريع للتطبيقات لبناء وتعديل التصميمات. أما بالنســبة لمشاريع التطوير السريــع للتطبيقات الأكبر حجماً، فإنه يجب تعيين المتخصصين كمديري قواعد البيانات، وفنيي الشــبكات ومبرمجي النظم ليكونوا مسؤولين عن القرارات الرئيسية المتعلقة بالتطوير السريع للتطبيقات RAD.
• لا بد من وجود معايير وضوابط للتطوير السريع للتطبيقات RAD في المؤسسة للتأكد من:
- أن الإدارات تستخدم أساليب التطوير السريع للتطبيقات RAD فقط إذا اقتضت الحاجة ذلك . - أن الإدارة تشتمل على الخصائص الأمنية والرقابية في جميع التطبيقات المطورة. - أن موظفي ضمان الجودة يقومون بفحص ما إذا كانت السمات الأمنية والرقابية (التي تتناسب مع مستويات المخاطر) موجودة وموظفة كما يجب أم لا. - أن المستخدمين النهائيين يشاركون بشكل مناسب خلال مشروعات التطوير السريع للتطبيقات RAD. - أن مديري المشروعات يراقبون عن كثب وعن قرب جميع أنشطة المشروع.
• قم بتحديد ما إذا كانت جميع التطبيقات التي تم تطويرها باســتخدام التطوير السريع للتطبيقات قــد تم توثيقها بالشــكل المناســب أم لا، وأن عملية التوثيــق قد تمت بالتوازي مــع عملية تطوير التطبيــق. ومن خلال الإنتاج المتزامن للوثائق ودون زيــادة الوقت المخصص لتطوير التطبيق، فإن التطبيقات المطورة بتقنية التطوير السريع للتطبيقات RAD ستسهم في توفير الوقت أثناء عمليات الصيانة المستقبلية للنظام.
• قم بوضع مبادئ صارمة فيما يخص قواعد التســمية أو كتابة الجمل البرمجية بحيث يتمكن مطور تطبيقات RAD بشــكل شــبه دائم مــن فهم نص شــيفرة المصــدر Source Code الخاصة بمولد التطبيقــات الــذي يتم توليده من قبل أحد محترفي التطوير السريــع للتطبيقات RAD أو غيره من محترفي تقنية المعلومات.

يمكننــا التأمل في وظائف نظام ERP من خلال عملية التصنيع، حيث يحتاج أحد أجزاء المنتج إلى تصميم، وطلب الموارد اللازمة لبناء هذا الجزء، ووضع العمليات الخاصة بحساب تكلفة وتســويق هذا الجزء، حيث يتم تنفيذ طلبات شراء المواد، وتبدأ عملية الإنتاج، ومن ثم يأتي دور التدفق الكلي لعمليات الإنتاج والعمليات التشغيلية فيما يتعلق باستقبال أوامر الــشراء من العميل، والشــحن، وإصدار الفواتير الخاصة بهذا العنــصر. إن هذه العمليات وغيرها تنطوي على سلسة من أنشطة مستقلة إلا أنها مرتبطة فيما بينها بعلاقات متبادلة،

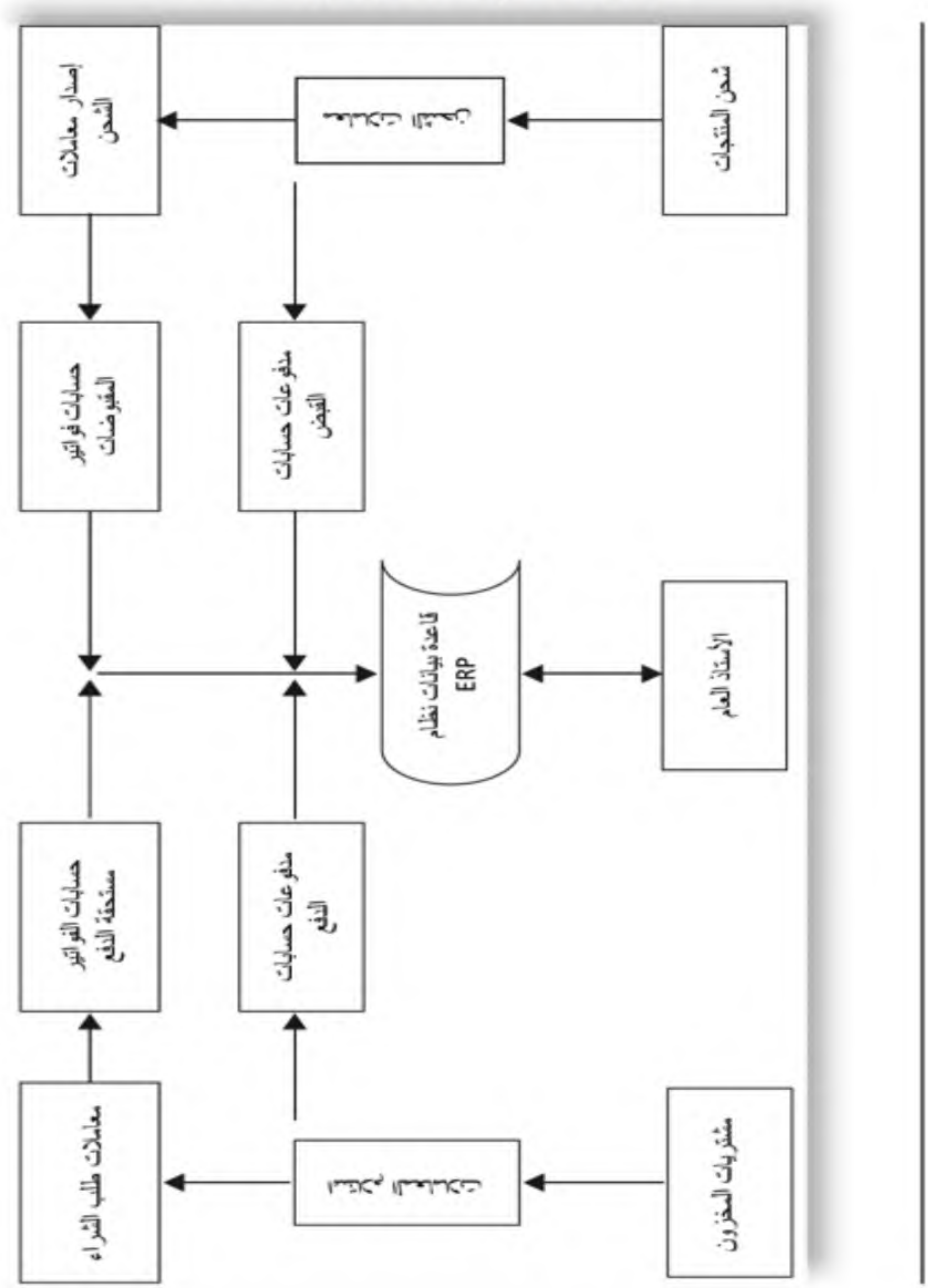
حيث كانت تدار في الســابق عن طريق مجموعــة منفصلة من تطبيقات تقنية المعلومات مثل التطبيقات الخاصة بتلقي الطلبات ومراقبة المخزون وجدولة الإنتاج والشحن وحساب المقبوضــات وغيرها الكثير. في حين يقوم نظام ERP بربط جميع هذه الأنشــطة وأكثر في سلسلة مترابطة بإحكام من وظائف قاعدة البيانات.

يحاول نظام ERP أن يعمل على تكامل كل الأقسام والإدارات في الشركة ليضعها في نظام حاسب آلي واحد يمكنه خدمة وتلبية الاحتياجات الخاصة بجميع الأقسام التابعة لها. وقد يكــون هذا أمــراً صعباً، أن يتم بناء نظام برمجي واحد يلبي حاجات الناس في الأمور المالية بالإضافة إلى الموارد البشرية والمستودعات. فقبل ظهور نظام ERP، عادة ما كان لكل قسم من هذه الأقسام نظام حاسب آلي خاص به مُطوَر بوسائل خاصة بحيث يستطيع القسم أن يقوم بأداء الأعمال الخاصة به، إلا أن نظام ERP قد قام بدمج هذه النظم جميعاً في نظام برمجي واحد متكامل يدار من قبل قاعدة بيانات واحدة، بحيث يســمح للأقسام المختلفة بمشــاركة المعلومات والاتصال فيما بينهم بســهولة. قد يكون لهــذا النهج التكاملي مردود واسع إذا ما قامت الشركات بتثبيت البرمجية بشكل سليم.

يوجد العديد من الطرق لوصف نظام ERP. إلا أن الشــكل التوضيحي (١٥-٥) يعرض لنا وصفاً لتدفق البيانات المحاســبية الأساسية الخاصة بأعمال إحدى المؤسسات. وتتضمن أوامر الشراء وحساب المدفوعات وغيرها من العمليات التقليدية لنظم الأعمال التي ستكون جــزءاً من نظــام ERP. هذه العناصر تعد مــن متطلبات النظم اللازمــة لبناء أحد أجزاء عملية التصنيع والتي تم وصفها مســبقاً. فقد كانت هذه العناصر عبارة عن عمليات نظم تقليدية منفصلة لكل منها بيانات وملفات معاملات رئيســية خاصة بها، وتستطيع الاتصال بتطبيقــات أخرى كنظام الأســتاذ العام. وعلى الرغم من أن هذا الشــكل يعرض سلســلة من عمليات توزيع الإنتاج كالوظائف التقليدية لحســاب المقبوضات، وحساب المدفوعات، فــإن التطبيق الكامل لنظام ERP الخاص بالمؤسســة يحتوى عــلى مجموعة أكبر بكثير من النظم الأخرى كالتســويق والموارد البشرية، إذ يتم ربط جميع النظم معاً بإحكام من خلال توصيفات وروابط مشتركة للبيانات.

شكل توضيحي (١٥-٥)

مثال على بنية نظام تخطيط موارد المؤسسة ERP



قد يتساءل المدير الأول عن سبب تأخير وصول معلومات شكاوى العملاء القادمة من نظام مرتجعات المنتجات. وقد يحتج أعضاء آخرون في الكادر الوظيفي من أنه يجب عليهم إعادة إدخال المعاملات نفسها في تطبيقات مختلفة ولكنها مترابطة. في أغلب الأحيان يبدو أن قاعدة البيانات المدمجة المشتركة - نظام ERP - هي الحل الأسهل هنا. من ناحية أخرى، فإن عملية تطبيق نظام ERP ليس بالخطوة السهلة أو الصغيرة. حتى في أحسن الظروف فإن هذا النظام سيستهلك كميات كبيرة من وقت وموارد المؤسسة. كما يجب أن يكون هناك مشاركة فعالة من المديرين الرئيسيين وأعضاء فريق تقنية المعلومات وحتى أصحاب المصلحة الآخرين.

من منظور حوكمة تقنية المعلومات فإنه يوجد نقاط رئيسية يجب أن يتم أخذها في الاعتبار عند تطبيق نظام قاعدة بيانات ERP في المؤسسة، وهي:

- **تحديد أهداف ومتطلبات نظام ERP:** يعتبر هذا المفهوم جديداً نسبياً في نظم تقنية المعلومات، إذ هناك الكثير من الدعاية المنشورة حول ما يمكن أن تحققه قواعد البيانات الشاملة لنظام تخطيط الموارد المؤسسية. فضلاً عن أنه بالاستناد إلى المعرفة التي لديهم فيما يمكن أن تحققه قواعد البيانات الشاملة لنظام تخطيط الموارد المؤسسية، يجب على المبادرين في المشروع وضع أهداف ومتطلبات قوية للمشروع الجديد الخاص بتطبيق نظام تخطيط الموارد المؤسسية ERP.
- **بناء فريق المشروع من جميع الإدارات:** إن قاعدة البيانات الخاصة بتخطيط موارد المؤسسة تعد أكثر من مجرد نظام جديد في تقنية المعلومات، وإنما ينطوي تحته العديد من أعضاء المؤسسة. لذا يجب تعيين فريق من جميع الوظائف المختلفة لتقنية المعلومات وأعضاء من مجتمع المستخدمين لقيادة المشروع القادم والخاص بتخطيط الموارد المؤسسية.
- **تقدير متطلبات التكلفة والوقت اللازمة لتطبيق نظام ERP:** بالنسبة للمؤسسة المكونة من وحدة أعمال واحدة فقط ويعمل بها ما بين ٢٥ إلى ١٠٠٠ موظف، قد تحتاج إلى حزمة أصغر من برمجية قاعدة بيانات ERP تُكلف نحو ٢٥٠٠٠٠ دولار أمريكي. في حين أن المؤسسات الكبيرة المتعددة وحدات الأعمال ويعمل بها عدد من المستخدمين

قــد يصل إلى ٥٠٠٠ مســتخدم، ربما يكلف البرنامج الأســاسي لنظــام ERP نحو مليوني دولار أمريــكي. كما يجب على المؤسســة أن تضع توقعات حقيقيــة وواقعية لمتطلبات الوقت اللازم لهذا المستوى من المشروع، وأن يفترضوا أن مثل هذا المشروع الكبير لتقنية المعلومات يحتاج إلى سنة واحدة على الأقل.

- **اختيــار أحد المنتجات البرمجية لنظام ERP:** هناك عدد كبير من الباعة يقدمون برنامج نظام تخطيط الموارد المؤسســية ERP. فهناك مزودو برمجيات رئيســيون أمثال ســاب SAP، أوراكل Oracle، وميكروسوفت Microsoft. هذا بالإضافة إلى بعض الباعة الأقل شــهرة مثل إيبيكور Epicor. ولتجنب سلســلة الاجتماعات أو اللقــاءات اللانهائية مع البائعــين والمواد الترويجية اللامعــة، فإنه يجب على الفريق المنوط بــه عملية الاختيار الوقــوف بحزم على الأهداف المحددة للمتطلبات والميزانية وعلى البيئة البرمجية الحالية للمؤسســة كذلك. ويتعين على أي بائع لمنتج برنامج ERP قابل للتطبيق أن يكون قادراً على تقديم نسخة تجريبية تمثل منتج ERP الخاص بهم.
- **تطبيق أســاليب منهجية لإدارة المشــاريع لتطبيق نظام ERP:** يتحدث الفصل السادس عــشر من هذا الكتاب عن تقنيات التخطيط الرســمية للمشــاريع والبرامج. ونظراً لأن تطبيق نظام ERP يعتبر مهمة كبيرة، فإنه يجب على المؤسسة أن تضع وتتبع منهجيات رسمية لتخطيط المشاريع من أجل تطبيق نظام ERP الذي نسعى إليه.
- **إنشــاء قاعدة بيانات تجريبية لنظام ERP والبــدء في التنفيذ المرحلي:** بمجرد أن يعمل تطبيــق ERP في المؤسســة عــلى أكمل وجه فإنه ســيؤثر في عدد كبير مــن التطبيقات التقليدية. على كل حال، يجب الحرص على إطلاق التطبيق المرحلي على أســاس تطبيق بعد الآخر، وذلك باستخدام قاعدة بيانات تجريبية أعدت في مراحل سابقة للمشروع.
- **تقديم تدريب مكثف للمستخدمين:** قد ينطوي التطبيق الجديد لنظام ERP على أشكال جديــدة للمعاملات وغيرها من التغــيرات التي تطرأ على النظــم والتي تكون في بعض الأحيــان صغيرة لكنهــا فنية. وفي جزء من خطة المشروع وفي إحدى مســئوليات أعضاء فريق تطبيق نظام ERP، يجب أن يكون هناك برنامج تدريبي قوي للمستخدمين.

- **إقرار ميزانيات المشرع ومراقبة حثيثة لتكاليف نظام ERP:** بعيداً عن رسوم الترخيص الخاصة بقاعدة البيانات التي تم اختيارها، فإن مشروع نظام ERP يعد من المشاريع الباهظة الثمن بالنسبة للمؤسسة. لذا يُطلب من أعضاء فريق المشروع وغيرهم من الأشخاص المشاركين في هذا العمل أن يقوموا بتسجيل عدد ساعات العمل الخاصة بهم فضلاً عن تحميل أي مصروفات مباشرة على مشروع نظام ERP. ولابد من مراقبة هذه المصروفات التي يتم تحميلها على المشروع ويتم المطالبة بها عن كثب والمساءلة بشأنها إذا اقتضى الأمر. في جميع الأحوال، ولعل أحد نقاط القلق الرئيسية بالنسبة لحوكمة تقنية المعلومات، والتي ربما تكون بمثابة مشكلة في بعض الأحيان عندما يقوم أعضاء الفريق بتحميل ساعات عملهم على المشروع حتى لو لم يقوموا بالفعل بتنفيذ أنشطة مرتبطة مباشرة بالمشروع.
- **وضع إستراتيجية للخروج إذا اقتضت الضرورة ذلك:** يمكن أن يسفر تطبيق نظام ERP الذي تم تخطيطه وتنفيذه بشكل جيد عن بعض المزايا الرئيسية الملموسة وغير الملموسة بالنسبة للمؤسسة. إلا أنه في بعض الأحيان قد تكون هناك أمور تسير على نحو خاطئ. على سبيل المثال، بعض سمات البرمجيات الخاصة ببائعي قاعدة بيانات ERP قد لا تعمل كما تم التعهد به أو كما كان متوقعاً. فقد يكون هناك مشاكل تقنية في شاشات النظم أو أي مجموعة أخرى من المشاكل المحتملة. فكما يقول التعبير القديم، لا تهدر المال الصالح في إصلاح ما تلف، فإنه يجب على فريق العمل أن يضع إستراتيجية خروج ليُنهي أعمال المشروع بشكل لطيف والعودة إلى العمليات التشغيلية التقليدية لتقنية المعلومات والأعمال.

شكل توضيحي (١٥-٦)

المزايا الملموسة وغير الملموسة الناتجة عن تطبيقات نظام ERP في المؤسسة.

المزايا الملموسة لنظام ERP:

- تخفيضات المخزون.
- تقليص أعداد الموظفين.
- تحسينات في إدارة النظام.
- تبسيط الروابط.
- تحسينات في دورة الإقفال المالي.
- تخفيض تكاليف تقنية المعلومات.
- تقليص تكلفة المشتريات.
- تحسينات في الإدارة النقدية.
- تقليل صيانة تقنية المعلومات والنظم.
- نظم محسنة تسلم في الوقت المحدد.

المزايا غير الملموسة لنظام ERP:

- وصول ورؤية أكبر لمعلومات النظم.
- عمليات محسنة جديدة.
- استجابات أكبر للعملاء.
- توحيد النظم والعمليات.
- تحسينات في سلسلة طلبات التوريد.

بالرغم من التصريحات التحذيرية الســابقة، فإن التطبيق الناجح لنظام ERP قد يعود على المؤسســة ببعض المزايا الملموسة وغير الملموسة. كما هو موضح في الشكل التوضيحي (١٥-٦). يمكن أن يكون تطبيق نظام ERP أحد المشروعات الكبيرة في المؤسسة والذي يمكن

أن يعود عليها بالعديد من الفوائد. وكما ناقشـــنا أهميـــة العمليات القوية لحوكمة تقنية المعلومات بالنســبة لكل من عمليات دورة حياة تطويــر النظم SDLC وعمليات التطوير السريع للتطبيقات RAD، فإن هذه القضايا تعد غاية في الأهمية عندما نقوم بإطلاق نظام قاعدة بيانات تخطيط الموارد المؤسسية ERP داخل المؤسسة.

الفصل السادس عشر
قضايا حوكمة تقنية المعلومات: إدارة المشاريع والبرامج

على الرغم من اســتخدام المؤسســات للهياكل التنظيمية الرسمية من أجل إدارة معظم الأنشــطة الخاصة بها، فإن هناك مجموعة كبيرة من أنشــطة المؤسســة التي يتم تنظيمها وإدارتها على شكل مشاريع. ويُستخدم مصطلح المشروع في الأنشطة العلمية، والحكومية، وحتى في الأنشطة المدرسية، وهو عبارة عن نشاط تعاوني يتم داخل المؤسسة ويشتمل على نشــاطات كالأبحاث أو تطوير نظم تقنية المعلومات. ويتم تخطيط المشاريع بشكل خاص من أجل تحقيق هدف معين على خلاف الأنشــطة الاعتيادية للمؤسسة. وتُعرف المشاريع عــادة بأن لها هيكلاً تنظيميــاً مؤقتاً وليس دائماً. وهي تتكون من فرق من داخل أو خارج الإدارات لإنجاز مهام محددة في أوقات محددة.

يتم تنظيم وإدارة العديد من أعمال تطوير نظم تقنية المعلومات على هيئة مشــاريع، فعندما تبدأ المؤسسة أو وحدة تقنية المعلومات التابعة لها في سلسلة من المشاريع المختلفة وفي الوقت نفســه يوجد بينها أوجه تشابه، فإن هذه المجموعات من المشاريع يطلق عليها اســم برامج Programs. وفي أغلب الأحيان تعد المشــاريع والبرامج وســائل فعالة لإدارة وتطبيق التغييرات التي تطرأ على نظم وعمليات تقنية المعلومات، إلا أنها قد تتسبب أيضاً في وجود بعض المشــاكل المتعلقة بالحوكمة والرقابة، وذلك لكونها مجهودات تتخطى عادة الحدود التنظيمية الاعتيادية، فهي تحتاج إلى آليات خاصة لمتابعة وضبط المشاريع.

سيتناول هذا الفصل التقنيات الفعالة لإدارة المشاريع والبرامج بهدف تحسين الحوكمة الشاملة لتقنية المعلومات. وسنقوم بتقديم المعايير الخاصة بالدليل المعرفي لإدارة المشاريع الصــادرة عن معهد إدارة Project Management Book of Knowledge (PMBOK) المشــاريع Project Management Institute (PMI) (www.pmi.org) كما ســنناقش أيضاً، لماذا يعد الامتثال لهذه المعايير من الأمور الهامة بالنســبة للإدارة الفعالة للمشــاريع والبرامج؟

عملية إدارة المشاريع:

يتـم اسـتخدام مصطلح المشروع غالباً على نحو غير سـليم هذه الأيـام في العديد من العمليات التشـغيلية الخاصة بتقنية المعلومات وغيرها من الأعمال المؤسسـية. فكثيراً ما يُطلب من مطوري تطبيقات تقنية المعلومات أو غيرهم من الأشخاص العاملين في مجالات أخـرى داخل المؤسسـة أن يقوموا بإعداد مـشروع لتنفيذ بعض الأعـمال المحددة. وكان المقصـود مـن الجهود الخاصـة بإعداد مثل هذا المـشروع والتخطيط له تخصيص أشـياء مختلفة لأشخاص مختلفين. وتقتضي هذه الجهود غالباً قيام القائد المعين باستدعاء الفريق المكلـف بالمـشروع للاجتماع وعمل ما هو أكثر بقليل من مجـرد قول، "أريدك أنت وأنت وأنت" لتنفيذ مهام المشروع المختلفة. ولم تكن الخطوات الضرورية اللازمة لتنظيم المشروع والتخطيط له تحظى بالاهتمام الكافي. ولهذا كانت هذه الجهود غير الرسـمية "للمشروع" تؤول غالباً إلى الفشـل بسبب عدم فهم الفريق المكلف بالمشروع لحقيقة الدور المنوط به وعـدم إلمامه بالأهداف العامـة للمشروع، هذا بالإضافـة إلى أن المتطلبات الخاصة بوقت ونطـاق المـشروع لم تكن محددة. وقـد أدت هذه الجهود في كثير من الأحيان إلى فشـل المشـاريع بسـبب تجاوز الوقت والميزانية أو للعديد من الأسباب الأخرى. كان سبب هذا الإخفاق غالباً هو الافتقار إلى نهج منظم ومتناغم لإدارة المشاريع.

وقد استمرت إدارة المشاريع في كونها مجرد مفهوم تم تعريفه بشكل ضعيف وغير واضح حتى منتصف تسـعينيات القرن الماضي. فعلى الرغم من وجود العديد من الأسـاليب الجيدة المعمول بها في ذلك الوقت في مشاريع البنية التحتية كبناء الجسور على الطرق السريعة، فإن تلك الحقبة قد شهدت العديد من الإخفاقات في تطوير نظم تقنية المعلومات. باستثناء بعض الأساليب التي كانت تقودها الولايات المتحدة الأمريكية لتحسين تلك المشاريع الخاصة بتطوير تقنية المعلومات، حيث لم يكن هناك نهج ثابت لإدارة المشاريع على مدى عدة سنوات. إلا أن الأمور قد تغيرت عندما تم تأسيس معهد إدارة المشاريع PMI، والذي بدأ بمجموعة صغيرة من المهنيين المتخصصين الأمريكيين الذين يبحثون عن تعريف أكثر انسجاماً مع أعمالهم. واعتباراً من عام ٢٠١٢ أصبح معهد إدارة المشـاريع PMI منظمة مهنية دولية تضم في عضويتها نحو ٦٠٠٠٠٠ شخص بين عضو ومدير مشاريع معتمد من قبل المعهد في ١٨٥ دولة. وقد قام معهد إدارة المشـاريع PMI ببحث وتطوير ونشر مجموعة كبيرة من المواد الإرشادية المتعلقة بإدارة

المشــاريع. ومن أهم المطبوعات الصادرة عن هذا المعهد الوثيقة الأشبه بالمعايير والتي أُطلق عليها كتاب الدليل المعرفي لإدارة المشــاريع PMBOK [1]. وهو بمثابة دليل لجميع الجوانب الخاصة بإدارة المشــاريع. وقد أصبح الدليل المعرفي لإدارة المشــاريع PMBOK أحد المعايير المهنية للممارسات الخاصة بإدارة المشاريع في جميع أنحاء العالم.

يعرض الشــكل التوضيحي (١٦-١) تعريف المشروع طبقاً للدليل المعرفي لإدارة المشــاريع PMBOK. وعــلى الرغــم من أن هذا الدليل يتســم إلى حد ما بالإســهاب وربما يكون عاماً وشــاملاً فقط للإرشــادات المتعلقة بحوكمة تقنية المعلومات، فإنه قام بتعريف المشروع على أنه جهد مؤقت له تاريخ بداية ونهاية معلوم وأهداف وغايات محددة. وتتخطى المشــاريع غالباً الحدود التنظيمية الاعتيادية وتعمل بشــكل منفصل نوعاً ما، أو خارج الإطار الطبيعي لإجراءات الإدارة أو المؤسسة. وقد يتم تخصيص فريق للمشروع مكون من أشخاص ينتمون إلى وحدات تنظيمية مختلفة في المؤسسة، ويتم تقديم التقارير على أساس الخط النقطي (نمط العلاقة الضعيفة بين الموظف ورئيســه) لمدير مشروع مســتقل. في بعض الأحيان، قد يعمل فريق عمل المشروع بدوام جزئي في المشروع مع استمرار تحملهم لمسؤولياتهم تجاه وظائفهم الاعتيادية. ونظراً لأن أنشطة المشروع تتخطى غالباً الحدود التنظيمية ويتم تشغيلها كأعمال منفصلة ومستقلة، ومن ثم قد تكون هناك مشاكل تتعلق بقضايا حوكمة تقنية المعلومات ما لم تكن هناك معايير قوية ومتسقة معمول بها لإدارة المشاريع.

إضافة للإرشــادات الخاصة بالدليل المعرفي لإدارة المشاريع والتي تتحدث عن المشاريع المستقلة القائمة بذاتها، فإن لدى معهد إدارة المشاريع PMI أيضاً المزيد من المواد الإرشادية والتوجيهيــة الخاصة بإدارة البرامج والمحافظ. وســيتم الحديث عنها في الأقســام اللاحقة. حيث تشــير إدارة البرامج بشــكل عام إلى سلسلة من المشــاريع المرتبطة ببعضها. في حين تشــمل إدارة المحافظ معايير خاصة بمجموعة المشــاريع والبرامج داخل المؤسسة. كما أن لدى معهد إدارة المشاريع PMI أيضاً برنامج الشهادة الاحترافية لمديري المشاريع، حيث يتم اعتــماد الأعضاء الذين يجتازون الاختبارات المهنية لهذا البرنامج بنجاح ويحققون متطلبات الخبرة كمدير مشروعات محــترف (PMP) Project Management Professional. وقد أصبح معهد إدارة المشــاريع PMI والدليل المعرفي لإدارة المشــاريع PMBOK الصادر عنه

من المعايير العملية بالنسبة للعديد من أنشطة إدارة المشاريع في المؤسسات سواء في الولايات المتحدة الأمريكية أم في جميع أنحاء العالم.

شكل توضيحي (١٦-١)

تعريف المشروع وفقاً للدليل المعرفي لإدارة المشاريع PMBOK

المشروع هو مسعى مؤقت يتم القيام به من أجل تقديم منتج أو خدمة أو نتيجة فريدة من نوعها. تشير الطبيعة المؤقتة للمشاريع إلى وجود بداية ونهاية واضحة. ويتم الوصول إلى النهاية عندما تتحقق جميع أهداف المشروع أو عندما يتم إنهاء المشروع بسبب عدم إمكانية تحقيق أهداف المشروع أو عندما لا يعود هناك حاجة إلى المشروع. وليس بالضرورة أن تشير كلمة مؤقت إلى فترات زمنية قصيرة. وعموماً فإن كلمة مؤقت لا تنطبق على المنتج أو الخدمة أو النتيجة التي حصلنا عليها من المشروع. ويتم القيام بمعظم المشاريع لخلق نتائج دائمة. على سبيل المثال، مشروع بناء تمثال أو نصب تذكاري وطني يؤدي إلى نتيجة من المتوقع أن تدوم لعدة قرون. وقد يكون للمشاريع أيضاً آثار اجتماعية واقتصادية وبيئية قد تدوم أكثر بكثير من المشاريع نفسها.

كما أن كل مشروع يعمل على إيجاد منتج أو خدمة أو نتيجة فريدة من نوعها. وعلى الرغم من احتمالية وجود عناصر مكررة في بعض مخرجات المشاريع، فإن هذا التكرار لا يغير سمة التفرد الأساسية لعمل المشروع. على سبيل المثال، يتم تشييد المباني المكتبية من المواد نفسها أو من مواد شبيهة وعن طريق الفريق نفسه، إلا أن كل موقع يختلف ويمتاز عن غيره في التصميم أو الظروف أو المقاولين أو غير ذلك.

إن جهود العمل المستمرة بشكل عام عبارة عن عملية متكررة، ذلك لأنه يسير وفق إجراءات تنظيمية قائمة. وعلى النقيض من ذلك، فإنه نظراً للطبيعة الفريدة للمشاريع، قد تحوم شكوكٌ حول المنتجات أو الخدمات أو النتائج التي يُوجِدُها المشروع. فقد تكون مهام المشروع جديدة بالنسبة لأعضاء فريق المشروع، الأمر الذي يتطلب تخطيطاً أكثر تفانياً من غيرها من الأعمال الروتينية. بالإضافة إلى ذلك، فإنه يتم تنفيذ المشاريع على جميع المستويات التنظيمية. وقد يشمل المشروع شخصاً واحداً أو وحدة تنظيمية واحدة أو وحدات تنظيمية متعددة.

يستطيع المشروع إيجاد:

- منتج يمكن أن يكون أحد مكونات عنصر ما أو عنصراً نهائياً بحد ذاته.
- القدرة على أداء خدمة (على أنها إحدى إدارات الأعمال التي تدعم الإنتاج أو التوزيع).
- أو نتيجة مخرج أو وثيقة (على سبيل المثال، أحد المشاريع البحثية التي تُستخدم لتحديد ما إذا كان هناك توجه معين أو عملية جديدة سوف تفيد المجتمع).

تقدم الأقسام التالية مقدمة عامة عن الدليل المعرفي لإدارة المشاريع PMBOK وأهميته باعتبارها أسـلوباً أساسـياً للتطوير وإدارة المشاريع. لسنا هنا بصدد تقديم وصف تفصيلي لمعايـير الدليـل المعرفي لإدارة المشـاريع PMBOK، بل تقديمها باعتبارهـا إحدى الأدوات الهامة لحوكمة تقنية المعلومات الخاصة بإدارة المشـاريع في المؤسسـة. عندما تقوم إدارة تقنية المعلومات في المؤسسة باستخدام تقنيات إدارة المشاريع لتطوير تطبيقات جديدة أو غيرها من عمليات النظم ، فلابد أن يتم هذا التطوير باستخدام أحد الأساليب المعتمدة في إدارة المشـاريع مثل PMBOK الخاص بمعهد إدارة المشاريع أو برنس٢ PRINCE2، وهو أيضاً أسلوب آخر هام جداً سنتحدث عنه في الأقسام اللاحقة.

معايير الدليل المعرفي لإدارة المشاريع PMBOK:

إن البحـث بواسـطة شـبكة الإنترنت عن موضوع إدارة المشـاريع سـينتج عنه آلاف المواضيـع التي تتناول جميـع القضايا والاختلافات المتعلقة بإدارة المشـاريع. أفضل تلك المراجع أو المواضيع الموجودة هذه الأيام هي التي تستند إلى الدليل المعرفي لإدارة المشاريع PMBOK الصـادر عن معهد إدارة المشـاريع PMI والذي يعد تقريباً الأسـلوب الفعلي والحقيقي الذي يصف جميع جوانب إدارة المشاريع. ونحن هنا بصدد تقديم نبذة عامة عن عمليات الدليل المعرفي لإدارة المشاريع PMBOK مع التركيز على أن يُعرف كيف يمكن أن يكون هذا الدليل مفيداً لتحسـين وتعزيز وظائف حوكمة تقنية المعلومات للأنشـطة الخاصة بإدارة المشاريع.

لقد تم تحديث معايير الدليل المعرفي لإدارة المشاريع بشكل منتظم، بحيث كانت تعتمد كل مجموعة جديدة من المواد الإرشادية على الإصدارات السابقة. تم إطلاق الإصدار الرابع للدليل المعرفي لإدارة المشـاريع في عام ٢٠٠٨. والذي يُعَرِّف إدارة المشاريع على أنها خمس مجموعات من العمليات الأساسـية وتسـعة مجالات معرفة، وهي تعتبر عناصر في جميع المشاريع تقريباً. ويمكن تطبيقها على المشاريع والبرامج والمحافظ وعمليات التشغيل. وقد أصبحت هذه المفاهيم بمثابة إطار عمل بالنسـبة لإطلاق وتنفيذ المشـاريع بفاعلية سـواء كانت مشاريع تقنية معلومات أو غيرها. المجموعات الخمس من العمليات الأساسية لإدارة المشاريع وفقاً للدليل المعرفي لإدارة المشاريع PMBOK هي:

١- **البدء:** لا بد من وجود عمليات رسـمية معمول بها لإطلاق أي مشروع. وتتضمن هذه العمليـات وصف أهداف المشروع والميزانية المتوقعة والموافقات المناسـبة. ويعد ذلك أحد المطالب الهامة لحوكمة تقنية المعلومات.

٢- **التخطيط:** كل مشروع بحاجة إلى تخطيط من حيث تقديرات الوقت والموارد المطلوبة بالإضافـة إلى الروابط بين المكونات والمشـاريع الأخرى التي تحتاج إلى تنسـيق. عملية التخطيـط للمشروع لهـا أهمية خاصة نظراً لأن معظم المشـاريع يتم تنظيمها وبناؤها خارج الحدود التنظيمية، ويشـكل لها فرق عمل مكونة مـن موارد متعددة من الموارد البشرية التي تعمل بدوام جزئي لبناء عناصر المشاريع.

٣- **التنفيذ:** تحدد هذه المجموعة من العمليات الأساسية الخاصة بالدليل المعرفي لإدارة المشاريع النشـاطات الفعليـة للمشروع. أي مـا الاحتياجات التي يجب الوفاء بهـا لتحقيق أهداف المشروع؟ من وجهة النظر الخاصة بتقنية المعلومات، فقد تمتد هذه النشاطات من البحث عن أدوات برمجية مناسبة إلى تفصيل برمجيات تتناسب مع متطلبات المستخدمين ومن ثم تنفيذ المشروع بعد إتمام عمليات اختبار الضوابط الداخلية المناسبة وتدريب المستخدمين.

٤- **التحكم:** وهو أحد المكونات الهامة في الحوكمة الشاملة لأنشطة المشروع. إذ لا بد من وجـود عمليات معتمدة ومعمول بها لمراقبة إتمام العناصر الأساسـية في المشروع والتي تعمل على تحديد ما إذا كانت الميزانيات والغايات قد تم تحقيقها أم لا.

٥- **الإغلاق:** تتطلب العملية الأخيرة إغلاق أعمال المشروع، ليأتي بعد ذلك تسـليم مكونات المـشروع وتلخيص نتائج المشروع وتقديـم تقارير بها. وبالعـودة إلى تعريفنا الرئيسي للمـشروع، فإن العمل أو المسـعى لا بـد أن يكون له نهاية محـددة يمكن أن يتم فيها تلخيص نتائج المشروع وأي خطوات تالية تم التخطيط لها للقيام بها مسـتقبلاً باستثناء الجهود المستقلة للمشروع.

يقوم الدليل المعرفي لإدارة المشاريع PMBOK بتوفيق أو مقابلة كل من هذه العمليات الخمس لإدارة المشـاريع مع تسـعة مجالات معرفة لإدارة المشـاريع من حيث مدخلاتها ومخرجاتهـا بالإضافـة إلى الأدوات والأسـاليب. حيث تتضمن مدخـلات المشروع الوثائق والخطـط والموارد اللازمة لإطلاق المشروع مع المخرجات المخطط لها، وبطبيعة الحال مواد

المشروع المكتمل. للانتقال من المدخلات الأولية للمشروع إلى المنتج النهائي الذي تم إنجازه، هناك حاجة ماسة لمجموعة واسعة من الأدوات والآليات الضرورية. فمشروع بناء منزل على سبيل المثال، سيكون بحاجة إلى خشب وخطة ولوازم أخرى كالمسامير ومواد التسقيف كمدخلات للمشروع. وتعتبر أيضاً المطرقة والمنشار ومعرفة النجارة من الأدوات الضرورية للبدء في البناء. وستكون نتيجة المشروع في هذا المثال البسيط هي المنزل الذي اكتمل بناؤه.

هناك ما هو أكثر تعقيداً بكثير من مجرد الحاجة إلى خشب أو مطرقة أو مسامير. فإطلاق العديد من مشاريع تنفيذ نظم تقنية المعلومات يتطلب تصريحاً واضحاً وصارماً بالأهداف، وخطة تفصيلية للمشروع، وخطط موارد، وخطط اختبار، والعديد من المواصفات التفصيلية الأخرى. كما يحتاج فريق تقنية المعلومات المخصص لبناء المشروع إلى فهم مجالات الاهتمام الخاصة بالمشروع؛ وأدوات كنظم الأجهزة المحمولة لتنفيذ وبناء وإطلاق عناصر ومكونات المشروع وكذلك أخصائيين على معرفة ودراية كافية في تقنية المعلومات لبناء وفحص وتنفيذ الأعمال. من عدة نواح، فإن بناء هيكل منزل يقطنه شخص يعد مشروعاً صغيراً وبسيطاً نسبياً مقارنة بالعديدَ من الأعمال الخاصة بالتطبيقات والبنية التحتية لتقنية المعلومات. فمعظم المشاريع التي يتم إطلاقها من قبل المؤسسات على اختلاف أنواعها تكون معقدة. وهذا التعقيد هو ما يضطرنا إلى اللجوء إلى معهد إدارة المشاريع PMI ومعايير أفضل الممارسات الموجودة في الدليل المعرفي لإدارة المشاريع PMBOK الصادر عنه. فقبل ظهور هذه المعايير، كانت المؤسسات في أغلب الأحيان تقوم بإطلاق الأعمال الرئيسية للمشروع دون أن يكون هناك تحضير واستعداد كاف. وكانت النتائج في الغالب عبارة عن تكاليف باهظة وتجاوزات في الوقت بالإضافة إلى الإخفاقات حتى في إتمام المشاريع. وقد كان لدى العديد من المشاريع التي لا علاقة لها بتقنية المعلومات المشاكل المؤسسية نفسها. فجميعها تفتقر إلى الأساليب الشاملة والمتسقة في إدارة المشاريع.

وقد عَرَفَ الدليل المعرفي لإدارة المشاريع PMBOK عملية إدارة المشاريع على أنها عملية تحدث بطريقة متناغمة وخاضعة للرقابة على نحو جيد. وبالإضافة إلى مجموعة عمليات إدارة المشاريع الخمس الأساسية، فقد حدد الدليل المعرفي لإدارة المشاريع PMBOK تسعة مجالات معرفة خاصة بإدارة المشاريع هي:

١- إدارة تكامل المشروع.

٢- إدارة نطاق المشروع.

٣- إدارة وقت المشروع.

٤- إدارة تكلفة المشروع.

٥- إدارة جودة المشروع.

٦- إدارة الموارد البشرية للمشروع.

٧- إدارة اتصالات المشروع.

٨- إدارة مخاطر المشروع.

٩- إدارة مشتريات المشروع.

ويصف الدليل المعرفي لإدارة المشاريع PMBOK كلاً من هذه المجالات المعرفية التسع بتفصيل معقول ومنطقي من حيث مدخلاتها وأدواتها ومخرجاتها. على سبيل المثال، وصف مجال المعرفة الخاص بإدارة وقت المشروع في الدليل المعرفي لإدارة المشاريع PMBOK يتضمن أقساماً خاصة بالمدخلات والأدوات والمخرجات لـ:

- **تحديد أنشطة المشروع:** وهي عملية تعريف إجراءات محددة يتم تنفيذها لإنتاج الملاحق أو المخرجات الفعلية للمشروع.
- **تسلسل أنشطة المشروع الحساسة:** لا بد من تحديد وتوثيق العلاقات الموجودة بين أنشطة المشروع.
- **تقدير الموارد الخاصة بالنشاط:** يجب تقدير أنواع وإعداد الأشخاص وكميات المواد والمعدات واللوازم المطلوبة لإتمام الأنشطة المجدولة للمشروع.
- **تقدير الفترات الزمنية للنشاط:** هناك ضرورة ملحة لتحليل تسلسل أنشطة المشروع والفترات الزمنية ومتطلبات موارد ووقت واحتياجات موارد المشروع، وذلك لجدولة أعمال ونشاطات المشروع.

• **وضع الجدول الزمني للمشروع:** إن خطة متابعة التقدم الذي يتم إحرازه تكون ضرورية لمراقبة حالة المشاريع لتحديث الإنجازات الخاصة بها وإدارة أي تغيرات قد تطرأ على الجداول الزمنية الخاصة بها.

هذه هي الخطوات الأساسية لإدارة الوقت بالنسبة لأي مشروع، وهي تعد بالتأكيد الأنشطة الرئيسية التي ينبغي على وحدة تقنية المعلومات في المؤسسة أخذها بعين الاعتبار عند قيامها بالتخطيط لمتطلبات الوقت لأي مشروع من مشاريع تقنية المعلومات.

بالإضافة للدليل الخاص بالإدارة العامة، فإن الدليل المعرفي لإدارة المشاريع (PMBOK) يحدد بشكل تفصيلي أدوات إدارة المشاريع وعملياتها اللازمة في كل مجال من من مجالات المعرفة التي أشرنا إليها. يلخص الشكل التوضيحي (١٦-٢) هذه العمليات وكذلك مجالات المعرفة الخاصة بالدليل المعرفي لإدارة المشاريع PMBOK. لا يهدف هذا الفصل إلى تقديم نظرة تفصيلية عن جميع عمليات ومجالات المعرفة الخاصة بالدليل المعرفي لإدارة المشاريع PMBOK، إنما يهدف إلى التركيز على الدور الذي يلعبه الدليل المعرفي لإدارة المشاريع PMBOK في التخطيط والتنفيذ للعمليات الفعالة الخاصة بإدارة مشاريع تقنية المعلومات. إذ تستند الأرقام المرجعية في الشكل التوضيحي (١٦-٢) إلى مواد الدليل المعرفي لإدارة المشاريع PMBOK، ولكن ما يهم هنا هو أن هذه الأرقام تؤكد الخطوات اللازمة لبناء مشاريع فعالة. على سبيل المثال، مجال المعرفة رقم ٧ عبارة عن إدارة تكلفة المشروع، وهي خطوات ضرورية لأي عملية من عمليات المشروع ويوضح الشكل التوضيحي (١٦-٢) مجموعات العمليات الضرورية، وهي تقدير التكاليف وبناء الميزانية والتحكم في هذه التكاليف.

أسلوب آخر لإدارة المشاريع: برنس٢ Prince2:

برنس٢ PRINCE2 هو أحد الأساليب الأخرى لإدارة المشاريع والمعترف بها بشكل قوي. وهو أسلوب معتمد على العمليات ومرتبط أكثر بالمواد الإرشادية الخاصة بإطار العمل آيتل الذي تحدثنا عنه في الفصل السادس من هذا الكتاب. وقد تم إطلاق الإصدار الأول من معيار PRINCE2 في عام ١٩٩٦ باعتباره طريقة أو منهجية عامة لإدارة المشاريع. وعلى الرغم من أنه لا يزال حتى الآن غير شائع الاستخدام في الولايات المتحدة، فإن أسلوب

PRINCE2 أصبـح مألوفـاً على نحو متزايـد بل ويعد هذه الأيام بمثابة الأسـلوب الفعلي لإدارة المشـاريع في كل من المملكة المتحدة ودول الاتحاد الأوروبي. إن PRINCE2 عبارة عـن أسـلوب معياري لإدارة المشـاريع يعتمد على العمليات فهو قائـم على مجموعة من المبادئ والعمليات المحددة لإدارة المشاريع. يصف الشكل التوضيحي (١٦-٣) عملية إدارة المشاريع وفقاً لمنهجية PRINCE2.

ومقارنة بالدليل المعرفي لإدارة المشاريع PMBOK، فإن منهجية PRINCE2 تعد أكثر توجهاً واعتماداً على حالة الأعمال من الدليل المعرفي لإدارة المشاريع PMBOK. ومن خلال هذه المنهجية أيضاً فإن إدارة المشاريع تكون موجهة نحو قيام الإدارة العليا بها أكثر من أن يقـوم بها فريق العمل المباشر. وتعد هذه المنهجية في كثير من النواحي أحد أفضل أدوات حوكمـة تقنية المعلومات فيما يتعلق بإدارة المشـاريع والإشراف عليها. ومع ذلك، فإننا لا نهدف من خلال هذا الفصل إلى وصف كيفية تطبيق منهجية برنس ٢ PRINCE2 لإدارة المشاريع، ولكننا نهدف فقط إلى تسليط الضوء عليه باعتباره أداة بديلة عن الدليل المعرفي لإدارة المشـاريع PMBOK للقيام بإدارة وضبط مشـاريع تقنية المعلومات. وينبغي على فريق الإدارة الذي يساعد في وضع ومراجعة ضوابط حوكمة تقنية المعلومات الخاصة بإدارة المشـاريع أن يُصر على ضرورة اتباع إدارة تقنية المعلومات لهذه المنهجيات الموضوعة فيما يتعلق بالتخطيط والإشراف على أنشطة المشاريع الخاصة بها. قد يستخدم العديد في هذه الأيام الدليل المعرفي لإدارة المشـاريع PMBOK والذي يتسـق مع الإدارة الفعالة لحوكمة تقنيـة المعلومات. عـلى كل حال، إذا كانـت إدارة تقنية المعلومات لم تقـم بعد باعتماد الدليل المعرفي لإدارة المشاريع PMBOK، فإن على الإدارة الأخذ بالنصيحة التي تحث على تبني وحدة تقنية المعلومات لمعايير PRINCE2 نظراً لأنها تتوافق بشـكل كبير مع أفضل ممارسات إطار العمل آيتل التي تناولناها في الفصل السادس من هذا الكتاب.

محفظة نظم تقنية المعلومات وإدارة البرامج:

يقـوم مديرو المشـاريع غالباً باسـتخدام مصطلح "برنامج" عندمـا يتحدثون عن عدة مشاريع. يكون البرنامج في العادة عبارة عن مشروع رفيع المستوى يُستخدم لإدارة سلسلة من المشـاريع المترابطة والمتصلة بعضها ببعض. على سـبيل المثال، قد ترغب المؤسسـة في

تنفيذ مبادرة كبيرة إلى حد ما، فيتم تقسيمها إلى سلسلة من المشاريع المنفصلة. ويستطيع كل مشروع من هذه المشـاريع العمل بشكل مسـتقل، غير أن هيكل البرنامج يقوم بإدارة جميع هذه المشـاريع معاً. ويسـتخدم هذا الفصل عموماً مصطلح "مشروع" للدلالة على عمـل أو جهد فـردي، ومصطلح "برنامـج" للدلالة على عدة مشـاريع مترابطة فيما بينها. وهنـاك مصطلـح آخر ألا وهـو محفظة اسـتثمارات تقنية المعلومـات Portfolio of IT Investments، والذي يشـير عادة إلى المكان أو المسـتودع الخاص باسـتثمارات المشاريع القائمـة. فعادة ما يتم تجميع عدة مشـاريع مترابطة بعضهـا مع بعض في برامج ومحافظ مشاريع.

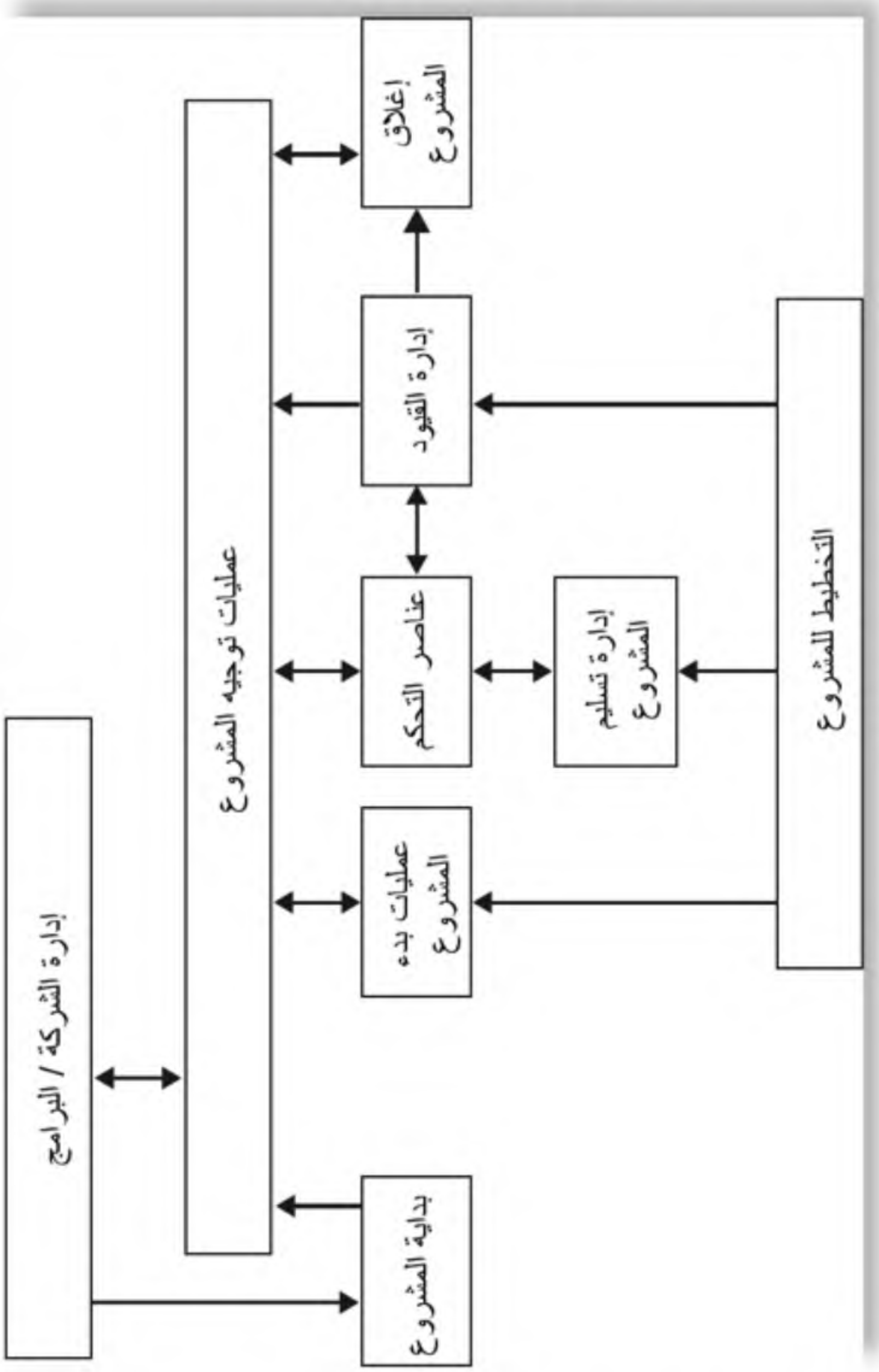
الشكل (١٦-٢)

موجز مجموعات العمليات ومجالات المعرفة الخاصة بالدليل المعرفي لإدارة المشاريع PMBOK

مجال المعرفة		مجموعات عمليات إدارة المشاريع: مجموعة عمليات البدء	مجموعة عمليات التخطيط	مجموعة عمليات التنفيذ	مجموعة عمليات المراقبة والتحكم	مجموعة عمليات الإغلاق
٤	إدارة تكامل المشروع	٤_١ وضع ميثاق المشروع	٤_٢ وضع خطة إدارة المشروع	٤_٣ توجيه وإدارة تنفيذ المشروع	٤_٤ مراقبة عمل المشروع ٤_٥ تنفيذ الرقابة المتكاملة للتغيرات	٤_٦ إغلاق المشروع أو المرحلة
٥	إدارة نطاق المشروع		٥_١ جمع المتطلبات ٥_٢ تحديد النطاق ٥_٣ وضع هيكل تجزئة العمل WBS		٥_٤ التحقق من النطاق ٥_٥ ضبط النطاق	
٦	إدارة وقت المشروع		٦_١ تحديد الانشطة ٦_٢ تقدير الموارد ٦_٣ تقدير موارد النشاط ٦_٤ تقدير الفترات الزمنية ٦_٥ وضع الجدول الزمني		٦_٦ ضبط الجدول الزمني	
٧	إدارة تكلفة المشروع		٧_١ تقدير التكاليف ٧_٢ تحديد الميزانية		٧_٣ ضبط التكاليف	
٨	إدارة جودة المشروع		٨_١ وضع خطة جودة	٨_٢ طبق ضمان الجودة	٨_٣ نفذ مراقبة الجودة	
٩	إدارة الموارد البشرية للمشروع		٩_١ وضع خطة الموارد البشرية	٩_٢ الحصول على فريق للمشروع ٩_٣ تطوير فريق المشروع ٩_٤ إدارة فريق المشروع		
١٠	إدارة اتصالات المشروع		١٠_٢ وضع خطة للاتصالات	١٠_٣ توزيع المعلومات ١٠_٤ إدارة توقعات المستفيدين	١٠_٥ إعداد تقرير الأداء	
١١	إدارة مخاطر المشروع		١١_١ وضع خطة إدارة المخاطر ١١_٢ تحديد المخاطر ١١_٣ إجراء التحليل الكمي للمخاطر ١١_٤ التحليل النوعي للمخاطر		١١_٦ المراقبة والتحكم بالمخاطر	
١٢	إدارة مشتريات المشروع		١٢_١ وضع خطة مشتريات	١٢_٢ متطلبات السلوك	١٢_٣ إدارة المشتريات	١٢_٤ إغلاق المشتريات

شكل توضيحي (١٦-٣)

عملية إدارة المشاريع وفقاً لمنهجية PRINCE2



يتكون برنامج إدارة المشـاريع من سلسـلة من المشـاريع المترابطة التـي تدار بطريقة متناسـقة للحصول على المزايا والضوابط التـي لا يمكن أن تكون متاحة في حال كانت هذه المشاريع تدار بشكل مستقل ومنفصلة بعضها عن بعض. حيث تتكون البرامج بشكل عام من عمل مترابط قد يكون خارج نطاق المشاريع المنفردة.

تظهـر الحاجة إلى إدارة البرنامج بشـكل عام عندما يكون لدى المؤسسـة هدف فردي محدد يمكن تحقيقه من خلال سلسلة من المشاريع المنفصلة. على سبيل المثال، خطة نقل منشـأة صناعية إلى موقع جديد، تتطلب وجود سلسلة من المشاريع المنفصلة التي بحاجة إلى تنسـيق. قد يتطلب أحد المشاريع هنا نقل وتركيب معدات الإنتاج، وقد يتطلب الآخر نقل المواد الخام، وسيبقى هناك مشروع آخر منفصل سيعمل على تغطية موضوع تحويلات نظم تقنية المعلومات. وعلى الرغم من أنه يجب أن يكون هناك شـخص ما يكون مسؤولاً عن تنسـيق جميع هذه الأعمال، فإن كل مشروع سيكون له احتياجاته ومتطلباته الخاصة. حيث سيتم إدارة هذه المشاريع بشكل منفصل ولكن بعد تجميعهم معاً كبرنامج واحد.

ينبغي على حوكمـة تقنية المعلومات النظر إلى متطلبات المشـاريع المترابطة والخاصة بتدقيق تقنية المعلومات على أنها برنامج. على سبيل المثال، قد يُطلب من المؤسسة مراجعة الضوابط الداخلية في مجموعة من المنشـآت وفقاً لقانون SOx البند ٤٠٤. حتى وإن كان كل مشروع من هذه المشـاريع المستقلة سـيتم تنفيذه على أنواع مختلفة من المرافق وفي مناطق جغرافية مختلفة وتحت مسـئولية فرق مختلفة في إدارة تقنية المعلومات؛ فإن كل مشروع من هذه المشاريع سيكون له الأهداف العالية المستوى نفسها، وقد يكون أحد كبار المديرين هو المسئول عن إتمام كل واحد من هذه المشاريع بشكل كلي. حيث يمكن تنظيم وإدارة هذه المجموعات من المشـاريع في برنامج، مع قيام كل مدير من مديري المشـاريع المسـتقلة بإعداد وإرسـال التقارير إلى مدير البرنامج من أجل تحقيق الامتثال العام لكامل العمل.

وبالانتقـال من مسـتوى إلى آخر أعلى، حيـث مصطلح إدارة المحافظ الذي يشـير إلى مجموعات من المشـاريع والبرامج والأعمال الأخرى التي يتم تجميعها معاً لتسهيل إدارتها على نحو فعال. في حال وجود مجموعات مستقلة لتقنية المعلومات في إدارتين داخل إحدى

الشركات، وربما تكون واحدة من هذه المجموعات مسؤولة عن العمليات التشغيلية للبنية التحتيـة لتقنيـة المعلومات في دول الاتحاد الأوروبي، في حين أن الأخرى مسـؤولة عن ذلك في الولايات المتحدة الأمريكية وكندا. في هذه الحالة يمكن اعتبار الأنشـطة الشاملة لتقنية المعلومـات لكل وحدة من الوحدات عبـارة عن حافظة (محفظة) لإدارة تقنية المعلومات، حيـث يمكن إدراج كلٍّ منهما تحت محفظة ذات مسـتوى أعـلى في المقر الرئيسي للشركة. إن هذه المفاهيم التي تتعلق بإدارة كل من المشـاريع والبرامج والمحافظ موضحة بالشكل التوضيحي (١٦-٤). الفكرة هي أن تلك العلاقات الواردة بالشكل يجب إنشاؤها إذا اقتضت الحاجة وذلك لتعزيز الكفاءة وتحقيق الأهداف العامة.

شكل توضيحي (١٦-٤)

نظرة عامة على إدارة المشاريع والبرامج والمحافظ.

	المشاريع	البرامج	المحافظ
النطاق	المشاريع لها أهداف محددة. سـيتضح النطـاق تدريجياً خلال دورة حياة المشروع.	البرامـج لهـا نطاقـات أكبر وتقدم مزايا أعظم.	المحافظ لها نطاق أعمال يتغير بتغير الأهداف الإسـتراتيجية للمؤسسة.
التغيير	يتوقع مديرو المشاريع التغيير ولذا يقومون بتنفيذ عمليات لإدارة التغيير والتحكم فيه.	يجـب على مديـري البرامج أن يتوقعوا التغيير سواء من داخل أو خارج البرنامج وأن يعدوا لإدارته.	يراقـب مديـرو المحافـظ باسـتمرار التغيرات في البيئة الواسعة.
التخطيط	مديرو المشـاريع بحاجة إلى التخطيط للتطور التدريجي مـن تخطيط عالي المسـتوى إلى تخطيـط تفصيلي خلال دورة حياة المشروع.	يضع مديـرو البرامج الخطة الشـاملة للبرنامج ويضعون خططـاً عاليـة المسـتوى لتوجيـه التخطيط التفصيلي على مستوى العنصر.	يقوم مديرو المحافظ بإنشاء العمليات والاتصالات الضرورية ذات الصلة بالمحفظة الإجمالية والإبقاء عليها.
الإدارة	يدير مديرو المشـاريع فريق المـشروع لتحقيـق أهداف المشروع.	يدير مديـرو البرامج أعضاء فريـق البرنامـج ومديـري المشـاريع. فهـم يقدمـون الرؤيـة وتكون لهـم ملكية البرنامج بالكامل	قـد يدير مديـرو المحافظ وينسقون أعضاء فريق إدارة المحفظة.

النجاح	يقاس النجـاح بجودة المنتج والمشروع وبالفترات الزمنية والالتزام بالميزانية وبمستوى رضا العملاء.	يقاس النجـاح بالدرجة التي عندها يتـم تحقيق البرنامج للاحتياجات والمزايا التي من أجلها تم وضع البرنامج.	يقاس النجاح من حيث الأداء الـكلي التجميعـي لمكونات المحفظة.
الرقابة	يقوم مديرو المشاريع بمراقبة وضبـط عمليـات تقديـم المنتجات والخدمات والنتائج التي أُقر المشروع من أجلها.	يراقب مديرو البرنامج التقدم التدريجـي لمكونات البرنامج لضـمان الالتـزام بـكل من الأهداف العامـة والجداول الزمنيـة والميزانيـة وتحقيق المزايا المرجوة.	يراقب مديرو المحافظ مؤشرات الأداء والقيمة التجميعية.

بالإضافة إلى مراجعة وإدارة المشـاريع والمحافظ الفردية لتقنية المعلومات، فإن الدليل الموضـح في الشـكل التوضيحي (١٦-٤) مفيـد لإدارة تقنية المعلومـات، حيث يوجد عدة مشـاريع متشـابهة لتدقيق تقنية المعلومات، والتي يمكن إدارتها كبرنامج أو اعتبارها جزءاً مـن محفظة مشـاريع. الفكـرة العامة هي أنه لا بد من أن يكون هنـاك تفاعل قوي بين البرامج أو المحافظ ومشـاريعهم المسـتقلة أو التابعة ، غير أن إدارة البرنامج لا تستطيع في الغالب أن توجه أو تملي شروطها على أنشـطة المشـاريع الفردية، كما أن المشاريع الفردية سـوف تسـاعد في تحديد البنية العامة للبرامج الداعمة. فالتشـابه بين سلسـلة عمليات التدقيق المستقلة لتقنية المعلومات وبين الإدارة العامة للتدقيق يكون قوياً للغاية.

إن العديد من إدارات تقنية المعلومات هذه الأيام محمّلة بالعديد من البرامج والمشاريع. حيث نجد أن بعض هذه المبادرات منظم على نحو جيد في حين يفتقر البعض الآخر للترابط الجيد حتى إنها تبدو عشـوائية. وكأحد العناصر الهامة في حوكمة تقنية المعلومات، يجب أن يكون هناك أعمال ومجهودات جارية ومستمرة لجعل إدارة تلك المبادرات الإستراتيجية الخاصة بالمشـاريع أبسـط وأكثر فاعلية. أما فيما يخص الحلول التي تقدمها حوكمة تقنية المعلومات في هذا الصدد فهو بناء أساس قوي لإدارة محافظ المشاريع. إن إدارة احتياجات المشـاريع ومواردها وميزانياتها على نحو فعال تعد بمثابة المفتاح الرئيسي لتقديم مبادرات تتعلـق بحوكمـة تقنية معلومات والتي تعمل على قيادة الشركة إلى الأمام وتصبح المسـار الصحيح الذي يساعد المؤسسة على تحقيق أهدافها.

مكتب إدارة البرامج (PMO)، أحد الموارد القوية للحوكمة:

كما تحدثنا سابقاً، فإن البرنامج عبارة عن مشروع ذي مستوى أعلى يعمل ليكون أداة للإدارة والإشراف على مشاريع أخرى، وهي المشاريع الفرعية. وقد بدأ ظهور هذا المفهوم في مجال تقنية المعلومات خلال سنوات استهلكت فيها أقسام تقنية المعلومات طاقاتها من أجل تسليم مشاريع مطلوبة في الوقت المحدد وفي حدود الميزانيات المخصصة. وقد كان الحل هو ضبط المشاريع بإحكام من خلال تأسيس ما يعرف بمكاتب إدارة البرامج Program Management Offices (PMO) باعتبارها وسيلة لتعزيز كفاءة تقنية المعلومات وخفض التكاليف وتحسين أداء المشاريع من حيث الالتزام بالوقت والميزانية. فما تم فعله لمشاريع تقنية المعلومات يمكن عمله تماماً على نحو جيد للمشاريع الأخرى في المؤسسة.

قد يقدم مكتب إدارة البرامج PMO المعايير أو سلطة الموافقة على جميع المشاريع أو حتى مهارات إدارة المشاريع وذلك من خلال كادر مكون من مجموعة من المحترفين المعتمدين في إدارة المشاريع. حيث تستطيع الوحدة الخاصة بمكتب إدارة البرامج PMO غرس الانضباط في إدارة المشاريع الذي تشتد الحاجة إليه في أقسام تقنية المعلومات وجميع المجموعات الأخرى المشاركة في إدارة المشاريع. كما يمكن لمكتب إدارة البرامج PMO المساعدة من خلال تقديم البنية اللازمة لتوحيد ممارسات إدارة المشاريع وتسهيل إدارة محافظ المشاريع بالإضافة إلى تحديد منهجيات لعمليات متكررة. ويعد قانون SOx - الذي يطالب الشركات بالإفصاح عن الاستثمارات، كالمشاريع الضخمة، التي قد تؤثر في الأداء التشغيلي للشركة - أحد العوامل المحفزة في هذا الصدد، فقد أجبر الشركات على عمل مراقبة حثيثة على نفقات المشروع ومدى تقدمه.

هناك نموذجان أساسيان لمكاتب إدارة البرامج PMOs: أحدهما يعمل بصفة استشارية حيث يزود مديري المشاريع في وحدات الأعمال بالتدريبات والإرشادات، وأفضل الممارسات. أما النموذج الآخر فيعمل على أنه مركز به مجموعة من مديري المشاريع يتم إعارتهم إلى وحدات الأعمال للعمل بصفةمديري مشاريع. إن الكيفية التي يتم بها تنظيم وإدارة مكتب إدارة البرامج (PMO) وتعيين الكوادر المؤهلة للعمل فيه تعتمد على عدد كبير من العوامل التنظيمية، من ذلك الغايات المستهدفة، ونقاط القوة التقليدية، والدوافع

الثقافيــة. فبتبني فكــرة وجود مكتب لإدارة البرامج (PMO) بمــا يتماشى مع ثقافة إدارة تقنية المعلومات، يمكن لمكتب إدارة البرامج PMO أن يساعد المؤسسة في القيام بالمشاريع الإســتراتيجية التي تُرضي كلاً من المســتخدمين الداخليين والخارجيــين. ومع مرور الوقت، يجب أن يكون مكتب إدارة البرامج PMO قادراً على تزويد المؤسســة بالفوائض المالية من خلال تفعيل إدارة أفضل للموارد وتقليص فشــل المشــاريع ودعم تلك المشاريع التي تعود على المؤسسة بفائدة أكبر.

تكــون مكاتب إدارة البرامج PMOs عادة عبــارة عن وحدات إدارية لدعم إدارة تقنية المعلومات، وقد تختلف هذه المكاتب من حيث أحجامها وبنيتها ومسؤولياتها. فهي تقدم إرشــادات في إدارة المشاريع لمديري المشــاريع في وحدات الأعمال وتعمل غالباً في مجالات الدعم التالية:

- **عملية / منهجية لإدارة المشاريع:** سواء كانت وحدة تقنية المعلومات في المؤسسة تستخدم الدليــل المعرفي لإدارة المشــاريع PMBOK أو برنــس٢ PRINCE2، فبإمكان مكتب إدارة البرامج PMO أن يقدم الإرشادات لتطوير وتنفيذ عمليات متناغمة وقياسية لإدارة المشاريع.
- **التدريب على إدارة المشــاريع:** وتعتبر هذه النقطة من المجالات الفعالة، حيث بإمكان مكتــب إدارة البرامــج PMO أن يقوم بعقــد برامج تدريبية تتعلق بالمشــاريع أو جمع متطلبات التدريب لكي تقوم بها شركة تدريب خارجية.
- **مقــر لمديري المشــاريع:** بما أن مكتــب إدارة البرامج PMO يعتــبر بمثابة مصدر مركزي للمعرفة والدعم اللازمين لإدارة المشــاريع، فبإمكانه الإبقاء على مكتب مركزي حيث يتم منه إعارة مديري المشاريع للخارج عند انتهاء المشروع المعين عليه.
- **الاستشــارات والتوجيهات الداخلية:** بهدف تشــجيع التميز في إدارة المشاريع، يستطيع مكتــب إدارة البرامــج PMO أن يقدم النصــح للموظفين الآخرين فيــما يتعلق بأفضل الممارسات مع التركيز على الدليل المعرفي لإدارة المشاريع PMBOK.
- **الأدوات البرمجية لإدارة المشاريع:** يمكن اختيار الأدوات البرمجية المخصصة لإدارة المشاريع وصيانتها لكي تستخدم من قبل جميع المشاركين في المشاريع، حيث يوجد العديد من المواد

البرمجية المتاحة لدعم أنشطة إدارة المشاريع. كما يمكن أن يعمل مكتب إدارة البرامج PMO بمثابة مركز لتبادل المعلومات فيما يتعلق باستخدام تلك الأدوات البرمجية.

- **إدارة المحفظة:** وضع فريق مكون من مديري المشاريع قادر على إدارة عدة مشاريع مترابطة مثل المشاريع الخاصة بتقنيات البنية التحتية، ومشاريع التطبيقات المكتبية وغيرها من المشاريع، وتخصيص الموارد وفقاً لذلك.

ربما توجد أساليب مختلفة لدى المنظمة للقيام بإدارة الوحدة الخاصة بمكتب إدارة البرامج PMO. لكن الطريقة المركزية التي تمتاز بالممارسة العملية على التحكم في المشاريع تكون غالباً أكثر فاعلية في المنظمات التي يتعامل فيها مكتب إدارة البرامج PMO بشكل نظامي مع كبار المديرين التنفيذيين ولديه كامل الصلاحية بإلغاء مشاريع أو وضع أولويات لها. فمن خلال استخدام منهجيات واضحة المعالم لإدارة المشاريع، فإن مكتب إدارة البرامج يمكنه غالباً العمل مع وحدات الأعمال في كل جانب من جوانب إدارة المشاريع ابتداءً من تحديد المتطلبات الرئيسية إلى المرحلة الخاصة بإجراء عمليات التدقيق التي تلي عملية التنفيذ. إن الإبقاء على عمليات متناغمة عبر المنظمة من شأنه أن يُمكِّن المنظمة من القيام بتجزئة المشاريع إلى مكونات أصغر يمكن إدارتها ومن ثم التقليل من الفشل.

تمتد مسؤوليات مكاتب إدارة البرامج PMOs بشكل واسع من توفير مركز لتبادل المعلومات المتعلقة بأفضل ممارسات إدارة المشاريع إلى إجراء المراجعات الرسمية لإدارة المحافظ. وليس من الضروري أن يقتصر إشراف مكتب إدارة البرامج فقط على تطوير المشاريع بل قد تشمل التنسيق وتتبع كلاً من المشاريع والخدمات. لذا يعد إنشاء مكتب لإدارة البرامج PMO للعمل في أي منظمة بمثابة تدريب على التكيّف وقوة التحمل. فعندما يتعلق الأمر بإنشاء مكتب لإدارة البرامج PMO، فإن هناك عدداً محدوداً من خرائط الطرق التي يمكن اتباعها، أو المعايير القياسية التي يسارع بتبنيها، أو المقاييس التي يمكن القياس على أساسها. إن أكثر مكاتب إدارة البرامج PMOs فاعلية هي تلك التي تجني التحسينات مع مرور الوقت وتدفع المنظمة دائماً إلى تحسين أدائها.

إدارة المشاريع ومكتب إدارة البرامج (PMO) وحوكمة تقنية المعلومات:

تقوم المؤسسات ببناء وتأسيس مبادرات تقنية المعلومات وغيرها من المبادرات الرئيسية الخاصة بها من خلال المشـاريع. وكما ذكرنا، فإن المشاريع وإدارة المشاريع الخاصة بتقنية المعلومـات تعمـل غالباً خارج الحـدود التنظيمية للمنظمة. فمبـادرة تنفيذ نظام جديد لحسـاب تكاليف الإنتاج مثـلاً، قد تحتاج إلى مـوارد من نظم وبرامج تقنيـة المعلومات، بالإضافة لأشـخاص من إدارة الحسـابات ووحدات الإنتاج المختلفـة. فعندما تكون هذه الجهـود خاضعة لإشراف مدير المشروع المعين، يمكن الحصول على الموارد واتخاذ الخطوات اللازمة لتنفيذ نظام حساب تكاليف الإنتاج المطلوب.

إن الاستخدام الفعال لمبادئ إدارة المشاريع يعد أحد العناصر الهامة في الحوكمة الفعالة لتقنية المعلومات. لذا يجب على إدارة تقنية المعلومات أن تتبنى منهجية لإدارة المشـاريع مثل الدليل المعرفي لإدارة المشـاريع PMBOK مثلاً. والأهم من ذلك، هو وجود ما يثبت أن جميع المشـاريع القائمة حالياً تستخدم هذا الأسلوب، وأنها تمتلك أساليب فعالة معمولاً بها في تخطيط المشـاريع، هذا بالإضافة إلى وجود مثل تلك الوثائق التي يعلن فيها صراحة عـن أهداف المشروع وخطط ضمان الجودة الموضوعة موضع التنفيذ. كما يجب أن يكون هناك دليل على وجود عمليات منهجية معمول بها لإدارة مشاريع تقنية المعلومات.

إذا كانت إدارة تقنية المعلومات تقوم باسـتخدام عمليات المشروع لبناء وإدارة العديد من أنشطته، وإذا كان هناك عدد كبير من المشاريع المترابطة، فعلى إدارة تقنية المعلومات أن تقوم بتأسيس مجموعة فعالة من العمليات الخاصة بمكتب إدارة البرامج PMOs. حيث تعد عملية إدارة البرامج أحد العمليات الهامة متى كان هناك عدد كبير من عمليات المشاريع المستخدمة في بناء وتنفيذ مشاريع وعمليات تقنية المعلومات. إن العمليات الفعالة في إدارة مشاريع تقنية المعلومات سوف تسهم في تحسين العمليات الشاملة في حوكمة تقنية المعلومات.

ملاحظة:

1- Project Management Institute, A Guide to the Project Management Book of Knowledge (PMBOK Guide), 4th ed. (Newtown Square, PA: 2008).

الفصل السابع عشر

اتفاقيات مستوى الخدمات (SLAs) ومنتدى إدارة خدمات تقنية المعلومات (itSMF) وقيمة تقنية المعلومات (Val IT) وتعظيم استثمارات تقنية المعلومات

منذ سنوات عديدة، تم تركيب نظم الحاسبات المركزية الأولى Mainframe في معظم الشركات الكبيرة. وكان ذلك بهدف تسيير العمليات التشغيلية والتقليل من التكاليف، وقد كان أحياناً بهدف إعطاء السمعة أو المكانة للشركات. وقد كان ذلك في الأيام الأولى عندما كانت تلك النظم المركزية الباهظة الثمن توضع في أغلب الأحيان في غرف زجاجية محكمة الإغلاق في أروقة داخل الشركات، وكان هناك توقعات كبيرة حول الفوائض التي ستعود على الأعمال جراء هذه التقنية الجديدة. لكن سرعان ما تبعها خيبة أمل كبيرة. ونظراً للمخاوف المتعلقة بموضوع الأمان والمساحة، فسرعان ما تم نقل تلك الأجهزة المركزية ومجموعة محركات الأشرطة والوحدات التخزينية المتزايدة الخاصة بها إلى مواقع بعيدة تابعة للشركة. والأهم من ذلك، كانت المدخرات الاستثمارية العائدة بطيئة نظراً للتكلفة الخاصة بتوظيف وبناء كادر من المتخصصين العاملين في تقنية المعلومات، وكذلك بسبب حالات التأخير والتكاليف المصاحبة للعديد من مشروعات تطوير تقنية المعلومات، وأيضاً بسبب البرامج التطبيقية التي لم تكن تعمل بالشكل الجيد كما هو متوقع. وسرعان ما أدركت المؤسسات أن هناك حاجة ماسة لمراجعة استثماراتها في مجال تقنية المعلومات الخاصة بها على جميع المستويات ومحاولة تحقيق المزيد من الفوائد الناتجة عنها.

يستعرض هذا الفصل القضايا والمخاوف المتعلقة بحوكمة تقنية المعلومات من عدة وجهات نظر فيما يتعلق باستثمارات المؤسسة في موارد تقنية المعلومات. وسوف نبدأ الحديث أولاً عن أهمية وضع اتفاقيات مستوى الخدمات SLAs وإدارتها على نحو فعال على أنها جزء من عمليات تشغيل تقنية المعلومات الخاصة بالمؤسسة. حيث تعد اتفاقيات مستوى الخدمة SLAs والإرشادات الخاصة بإدارة الخدمات المرتبط بها واحدة من أفضل الممارسات الخاصة

بإطار العمل آيتل التي تم تقديمها للمرة الأولى في الفصل السادس من هذا الكتاب. وهي عبارة عــن مجموعة من التفاهمات أو العقود الداخلية بين مســتخدمي خدمــات تقنية المعلومات وإدارة تقنية المعلومات. فهي تصف الخدمات التي ستقدمها وحدة تقنية المعلومات للإدارات المختلفة للمستخدمين وتشــمل الملفات والتقارير المحدثة، إضافة إلى تسليم الملفات والوثائق المحددة في الوقت المناسب. كما سنؤكد أهمية اتفاقيات مستوى الخدمة SLAs على أنها إحدى الأدوات الهامة لحوكمة تقنية المعلومات وسنتحدث أيضاً عن كيفية تطبيق هذه الاتفاقيات في المؤسسة وحصد المزايا والفوائد الناتجة عنها على نحو أكثر فاعلية.

المنتدى الذي يمكن اعتباره مرتبطاً ارتباطاً وثيقاً بإطار العمل آيتل لكنه مستقل عنه، هو منتــدى إدارة خدمات تقنية المعلومــات IT Service Management Forum (itSMF). وهو عبارة عن منظمة ذات عضوية مهنية مستقلة قامت بتعزيز وترويج العمليات الخاصة بــإدارة خدمات تقنية المعلومات ونشرت بعض الإرشــادات التي لها علاقة بهذه المجالات. فمن خــلال الفروع المحلية في العديد من المدن الرئيســية ومع الاهتــمام القوي والمتزايد بقضايــا حوكمة تقنية المعلومــات. فإن منتدى إدارة خدمات تقنية المعلومات itSMF هو المنظمــة التي ربما يهتم بها محترفو الإدارة لمزيد من البحث والاستكشــاف. ســيقدم هذا الفصل هذه المجموعة الاحترافية ويســلط الضوء عــلى بعض نقاط القوة المتعلقة بحوكمة تقنية المعلومات الخاصة بها.

سيقدم هذا الفصل أيضاً بشكل موجز ما يُعرف بالمجموعة المفتوحة للامتثال والأخلاقيات Open Compliance and Ethics Group (OCEG) ومعايــير الحوكمة وإدارة المخاطر والامتثال GRC الخاصة بها.

كما ســيقدم هذا الفصل أيضاً بعــض التفاصيل الإضافية عن معايــير الحوكمة الخاصة بهــذه المجموعــة مع التركيز على "الكتــاب الأحمر" الخاص بهــذه المجموعة. ومن المؤكد أننا ســنلاحظ التركيز المتزايد على المعايير الخاصة بالمجموعة المفتوحة للامتثال والأخلاقيات OCEG باعتبارها أدوات تســتخدم لتحسين حوكمة تقنية المعلومات في السنوات القادمة. وسيناقش هذا الفصل بعض المعايير والأدوات التي صدرت عن منتدى إدارة خدمات تقنية المعلومات لتحسين كل من حوكمة تقنية المعلومات ومخاطر الأعمال والاحتيال.

قامــت جمعية تدقيــق وضبط نظم المعلومــات (ISACA) التي تــم تقديمها في فصول ســابقة بتطوير وإصدار مجموعة من المواد الإرشــادية التي أطلق عليها مصطلح قيمة تقنية المعلومات Val IT التي تهدف إلى فهم وتقييم الاســتثمارات التي خصصتها المؤسســة لموارد تقنية المعلومات لديها على نحو أفضل. كما ســيقوم هذا الفصل بتقديم نموذج قيمة تقنية المعلومات Val IT وســيوضح لمــاذا يعد هذا النموذج واحداً مــن المفاهيم الهامة التي من الممكن أن تساعد الإدارة العامة وإدارات تقنية المعلومات التابعة لها في العمل سوياً على نحو أفضل بهدف تحقيق قيمة أكبر من عمليات تقنية المعلومات الخاصة بهم.

ســيُختَتَم هذا الفصل ببعض الإرشــادات العامة بالنســبة للمؤسسة فيما يتعلق بقياس وتحقيق القيمة المكتســبة من اســتثمارات تقنيــة المعلومات الخاصة بهــا. إننا مع مرور الوقت أصبحنا أكثر ذكاءً، وذلك عندما تلاشت بشكل كبير نظم الحاسبات المركزية الضخمة والمكلفــة. وأصبحنــا الآن نقوم وفي فترات زمنية صغيرة بتجميــع التطبيقات الجديدة من قائمة الخيارات الموجودة في نظام قائم على السحابة بدلاً من بناء تلك التطبيقات داخلياً من قبل طاقم التطوير الموجود في المؤسسة. ومع ذلك فإن المؤسسة بحاجة إلى معرفة تكاليف تلك النظم واتخاذ التدابير والإجراءات المناســبة لتحقيق أكبر قيمة ممكنة. ويعد ذلك من العناصر الهامة في حوكمة تقنية المعلومات.

أفضــل ممارســات إدارة الخدمــات طبقاً لإطار آيتــل ومنتــدى إدارة خدمات تقنية المعلومات (ITSMF):

ســبق الحديــث في الفصل الســادس من هــذا الكتاب عن مكتبــة البنية التحتيــة لتقنية المعلومــات آيتل (ITIL) وعن معايير أفضل الممارســات الخاصة بهــا، وذلك فيما يتعلق بدعم وتقديم خدمات تقنية المعلومات. فهي تقوم بتوفير الإرشــادات والدعم الفعال لكل من إدارة تقنية المعلومات في المؤسسة والعديد من المجالات المتعلقة بحوكمة تقنية المعلومات، فعمليات مكتبة البنية التحتية لتقنية المعلومات آيتل تغطي مجالات أكثر توافقاً مع عملية التشغيل التي تتســم بالسلاسة للبنية التحتية الشــاملة لتقنية المعلومات. وعلى الرغم من إلقاء الضوء عليها مع العمليات الأخرى لأفضل الممارســات في الفصل السادس من هذا الكتاب، فإن فهم وتطبيق أفضل ممارسات إدارة مستوى الخدمات في آيتل يعد أمراً في غاية الأهمية خصوصاً هذه الأيام.

إن إدارة مســتوى الخدمــة Service level management هو الاســم المُعطى لعملية التخطيط، والتنســيق، والصياغــة، والاتفاق، والرقابة، وإعــداد التقارير فيما يخص الاتفاق الرســمي بين كل من إدارة تقنية المعلومات في المؤسســة ومقدمي ومتلقي خدمات تقنية المعلومــات. وتأخــذ هذه العمليــات الصفة الرســمية من خلال إبرام اتفاقيات مســتوى الخدمــات SLAs بــين تقنية المعلومات والعملاء أو المســتخدمين للتطبيقــات والعمليات والخدمات الأخرى الخاصة بتقنية المعلومات. أي أن هذه الاتفاقيات تمثل الاتفاق الرسمي بــين مقدمي خدمــات تقنية المعلومات وعملاء تقنية المعلومــات. عندما تم نشر الإصدار الأول للمواد الخاصة بأفضل ممارسات مستوى الخدمة في آيتل عام ١٩٨٩، كانت اتفاقيات مســتوى الخدمة SLA من المفاهيم المثيرة للاهتمام، إلا أنها لم تكن شائعة في ذلك الوقت. أما في الوقت الراهن فقد قامت العديد من المؤسسات بطرحها بالرغم من تفاوت درجات نجاحهــا، ويتعين على كبار المديريــن أن يكونوا على دراية كافية بها ومدركين لأهميتها عند فهم الضوابط الداخلية للبنية التحتية لتقنية المعلومات.

وفي مثــال على اتفاقيات مســتوى الخدمة، عندما تقــوم إدارة تقنية المعلومات في المؤسســة بالتعاقد مع مقدم خدمات خارجي على تقديم بعض الخدمات، مثل خدمة النســخ الاحتياطــي الخاص بالتعافي مــن الكوارث، فإنه لا بد مــن تأمين وحماية هذه الاتفاقيــة من خلال عقد رســمي يتم مــن خلاله الحصول على موافقــة مقدم خدمة التعافي من الكوارث على تقديم مســتويات معينة من هذه الخدمة وفقاً لجدول زمني محــدد يعتمد على وقت الاســتجابة. وفي هذه الحالة يُطلق عــلى العقد المنظم لهذا الاتفاق اسم اتفاقية مستوى خدمة SLA بين وحدة تقنية المعلومات ومقدم الخدمات المســتمرة. وفي هذه الحالة تكون اتفاقيات مســتوى الخدمة SLAs المبرمة بين إدارة تقنية المعلومات وعملائها أكثر أهمية من منظور الرقابة الداخلية. لقد قمنا باستخدام مصطلح "العميل" للدلالة على المصطلح القديم الذي لا يزال شــائعاً حتى الآن ألا وهو "مســتخدمو تقنية المعلومات". كما أن هناك مجموعات كثيرة في المؤسســة تستخدم مصطلــح "خدمات تقنية المعلومــات" IT's Services، وباعتبارهم عملاء لإدارة تقنية المعلومــات، فإنهم يتوقعون مســتويات معينة من الخدمة والاســتجابة. ويتم تحديد وتعريــف هــذه الاتفاقيات من خلال ما يُعرف باتفاقية مســتوى الخدمة SLA، وهي

عبـــارة عن اتفاق موثق بين إدارة تقنية المعلومات وعملائها يحدد الأهداف الرئيســـية للخدمات والمســـؤوليات المنوطة بكلا الطرفـــين. لذا لابد من التركيز على الاتفاقية، كما لا يجب أن تســـتخدم اتفاقيات مســـتوى الخدمة وســـيلة لتهديد طرف أو آخر لإجباره على الاســـتجابة لمطالبه. نحن أيضاً لا نتحدث هنا عن وجود ضرورة رســـمية أو شكل قانـــوني للوثيقة، ولكن نتحدث عن تفاهم موثق بـــين جميع الأطراف. لذلك لا بد من عمـــل شراكة حقيقية بين مقدم خدمات تقنية المعلومات والعملاء للتوصل إلى اتفاقية ذات منفعة متبادلة. خلاف ذلك، ســـتفقد اتفاقية مســـتوى الخدمة أهميتها بشـــكل سريـــع وتكون هدفاً لتلقي اللوم وقد تمنع ثقافة إلقاء التهم في هذه الحالة حدوث أي تحسينات حقيقة على جودة الخدمات.

بنـــاء على اتفاقية مســـتوى الخدمة، تتعهـــد إدارة تقنية المعلومـــات بتقديم خدمات محددة طبقاً لكل مجموعة من الجداول الزمنية المتفق عليها، وعليها أن تتفهم أن هناك عقوبـــات جزائية إذا لم يتم تحقيق معايير الخدمة. إن الهدف من كل هذا هو المحافظة على جودة الخدمات وتحســـينها من خـــلال دورة ثابتة من الاتفـــاق، والمتابعة، والإبلاغ، وتحســـين المســـتويات الحالية لخدمات تقنيـــة المعلومات. لذا يجـــب أن تركز اتفاقيات مستوى الخدمة بشكل إستراتيجي على الأعمال والحفاظ على المواءمة بين الأعمال وتقنية المعلومات.

يلخص الشـــكل التوضيحي (١٧-١) محتويـــات الاتفاقية النموذجية لمســـتوى الخدمة. وننـــوه هنا إلى أنه لا يجب أن تكون هذه الاتفاقية عبارة عن نوع من الوثائق التي تشـــبه وثيقـــة رهـــن منزل يتم التوقيع عليها على أنها جزء من عمليـــة إتمام شراء المنزل، بل ليقوم عملاء تقنية المعلومات باستخدامها في توثيق متطلبات خدمة تقنية المعلومات التي يسعون إليها مثل "ألا يزيد متوســـط وقت الاســـتجابة عن ..." أو " المعالجة الخاصة بإقفال النظم الماليـــة تتم بحلول ... " أو غيرها من العوامـــل. ولضبط التوقعات الخاصة بتلك الخدمات وعـــرض ما يمكن أن يكون متاحاً منها، فـــإن إدارة تقنية المعلومات تقوم عادة بتقديم بيان خاص بعروض خدمات تقنية المعلومات. لذا يجب إتمام التفاوض بشأن المتطلبات الخاصة بعملاء خدمات تقنية المعلومات ووضعها في اتفاقيات رســـمية لمستوى الخدمة. كما يجب

مراقبة الأداء في مقابل هذه الاتفاقيات الخاصة بمستوى الخدمة بشكل مستمر وإرسال تقارير تتعلق بأدائها بشكل منتظم. حيث إن الإخفاق في تحقيق المعايير الخاصة باتفاقية مستوى الخدمة قد يؤدي إلى المزيد من المفاوضات والتعديلات المتعلقة بهذه الاتفاقية. وتوفر هذه العملية الخاصة باتفاقية مستوى الخدمة فوائد ومزايا لكل من الأعمال ووحدة تقنية المعلومات تشمل ما يلي:

- نظراً لأن وحدة تقنية المعلومات يجب أن تعمل على تحقيق المعايير التي تم التفاوض بشأنها، فإن خدمات تقنية المعلومات تميل إلى أن تكون ذات جودة أعلى، الأمر الذي يؤدي إلى أعطال أقل. ومن الواجب أيضاً أن تتحسن إنتاجية مستخدمي تقنية المعلومات.
- سيتم استخدام الموارد البشرية في تقنية المعلومات بشكل أكثر فاعلية عندما تقوم وحدة تقنية المعلومات بتقديم الخدمات التي تلبي التوقعات الخاصة بالعملاء بشكل أفضل.
- باستخدام اتفاقيات مستوى الخدمة، يمكن قياس الخدمات المقدمة وسيتحسن عموماً التصور الخاص بعمليات تشغيل تقنية المعلومات.
- إن وجود العقود الملزمة سيجعل الخدمات المقدمة من الأطراف الأخرى (طرف ثالث) أكثر قابلية للإدارة ويقلل أي احتمالية للتأثير السلبي على خدمات تقنية المعلومات التي يتم تقديمها.
- إن مراقبة جميع خدمات تقنية المعلومات الخاضعة لاتفاقيات مستوى الخدمة تساعد على تحديد نقاط الضعف التي يمكن تحسينها.

شكل توضيحي (١٧-١)

عينة لمحتويات اتفاقية مستوى خدمات تقنية المعلومات

نظراً لعدم وجود نموذج أو صيغة موحدة لاتفاقية مســتوى خدمات تقنية المعلومات، فلا بد من أخذ العناصر التالية في الاعتبار على أنها محتوى لمعظم اتفاقيات مستوى الخدمات:
صفحات مقدمة الاتفاقية: • الأطراف المشاركة في الاتفاقية. • عنوان الاتفاقية ووصف بسيط عنها. • تواريخ: البداية والنهاية، والمراجعة. • نطاق الاتفاقية، الأمور المشمولة وغير المشمولة. • مسؤوليات كل من مقدم الخدمة والعميل. • وصف للخدمات المشمولة.
ساعات الخدمة Service hours: • الوقت الطبيعي اللازم لكل خدمة. (مثال ٢٤x٧ أو من الاثنين إلى الجمعة من الساعة ٨:٠٠ -١٨:٠٠). • الترتيبــات الخاصــة بطلبات مد الخدمة متضمناً ذلك فترات الإشــعار المطلوبة. (مثال: يجب أن يتم تقديم الطلب إلى مكتب الخدمة قبل حلول الثانية عشرة ظهراً لتمديد الخدمة في التوقيت المسائي، وقبل الثانية عشرة ظهراً يوم الخميس لتمديد الخدمة خلال عطلة نهاية الأسبوع). • فترات سماح لساعات خاصة (مثل: الإجازات العامة). • التقويم الزمني للخدمة.
الإتاحة Availability: • مســتويات الإتاحة المســتهدفة ضمن الســاعات المتفق عليها. ويتم التعبير عنها عادة بالنسب المئويــة. لــذا يجب تحديد فترة وطريقة القياس والتي يمكــن أن تعبر عن كامل الخدمة أو الخدمات الداعمة أو المكونات الحساســة أو الثلاثة معاً. ونظراً لصعوبة ربطها بالنســب المئوية المبسطة، فإنه يمكن قياس الإتاحة من حيث عدم قدرة العميل على تنفيذ أنشطة الأعمال الخاصة بالخدمة.

موثوقية الخدمة Reliability: • يتــم التعبــير عنها عادة بعــدد انقطاعات الخدمة أو بمتوســط الوقت بين الأعطال Mean Time Between Failures (MTBF) أو بمتوســط الوقــت بــين حوادث النظم Mean Time Between System Incidents (MTBSI).
الدعم Support: • ساعات الدعم (وهي تختلف عن ساعات الخدمة) متضمناً ذلك الترتيبات اللازمة لتقديم طلبات تمديد الدعم. • فترات الإشعار المطلوبة (مثلاً: يجب تقديم الطلب الخاص بتمديد الخدمة خلال الفترة المسائية إلى مكتــب الخدمة قبــل الثانية عشرة ظهــراً أو قبل الثانية عشرة ظهراً يــوم الخميس لتمديد الخدمة خلال فترة عطلة نهاية الأسبوع). • فترات سماح لساعات خاصة (مثل: العطل والإجازات العامة). • الوقت المستهدف للاستجابة للحوادث سواء كان مادياً أم باستخدام وسائل أخرى (مثال: الاتصال الهاتفي أو بالبريد الإلكتروني). • الوقــت المســتهدف لحل الحوادث، وذلك في حدود أولوية كل حــدث — حيث يختلف الهدف اعتماداً على أولوية الحوادث.
الطاقة الإنتاجية Throughput: • هــي مؤشر على حجم الحركة والأنشــطة الإنتاجية المحتملة. (مثال: عــدد المعاملات التي يتم تنفيذها أو عدد المســتخدمين الذين يعملون في الوقت نفســه او حجم البيانات التي يتم نقلها عبر الشبكة).
أوقات الاستجابة للمعاملات Transaction response times: • الأوقات المستهدفة لمعدل أو أعلى وقت استجابة لمحطة عمل. (أحياناً يتم التعبير عنها باستخدام النسب المئوية كأن نقول ٩٥٪ في غضون ثانيتين).
الأوقات المطلوبة لتبادل الدفعات Batch turnaround times: • أوقات تقديم المدخلات وزمان ومكان تسليم المخرجات.

التغيرات Changes: • أهـداف تخـص الموافقة عـلى طلبـات التغيـير Request For Changes (RFCs) ومعالجتها وتنفيذها، والتي تعتمد عادة على الفئة أو إلحاحية/ أولوية التغيير. • استمرارية وأمن خدمات تقنية المعلومات IT service continuity and security • الإشـارة باختصار لخطط اسـتمرارية خدمات تقنية المعلومات وكيف يتم اسـتدعاؤها وتغطية أي قضية من القضايا وخصوصاً أي مسـئولية من مسـئوليات العميل. (مثال: النسخ الاحتياطي لأجهزة الحاسبات الشخصية المستقلة PCs وتغيير كلمات المرور). • تفاصيـل تتعلق بأي أهداف تخص الخدمات التي يتم الاسـتغناء عنها أو تعديلها في حال وقوع كوارث (إن لم يكن هناك أي اتفاقية منفصلة لمستوى الخدمة فيما يتعلق بموقف كهذا).
المطالبات المالية Charging: • تفاصيـل عن الصيغـة أو المعادلة formula الخاصة بالمطالبات الماليـة والفترات الزمنية لها (في حال كانت هناك مطالبات مالية). إذا كانت اتفاقية مستوى الخدمة تشمل العلاقة مع المصادر الخارجيـة التي يتم الاسـتعانة بها، فإنه يجب تفصيـل المطالبات الماليـة في الملحق كونها يتم تغطيتها غالباً بأحكام المعلومات السرية.
إعداد تقارير عن الخدمات ومراجعتها Service reporting and reviewing: • محتوى، وتكرار، وتوزيع تقارير الخدمات وتكرار اجتماعات مراجعة الخدمة.
الحوافز/ الجزاءات المرتبطة بالأداء Performance incentives/penalties: • تفاصيل عن أي اتفاقية تتعلق بالحوافز أو الجزاءات المالية اعتماداً على الأداء مقابل مسـتويات الخدمـة المحـددة. وعلى الأرجح أن يتم تضمين هذه المعلومـات (الحوافز/ الجزاءات) في حال كانت الخدمات تقدم عن طريق منظمة خارجية (طرف ثالث). ومن الجدير بالذكر هنا هو أن الشروط الجزائية يمكن أن تتسبب بوجود صعوبات خاصة بها.

إن عملية إبرام اتفاقية مسـتوى الخدمة هي إحدى العناصر الهامة لعمليات تشـغيل تقنية المعلومات. فإذا لم تكن المؤسسـة تسـتخدم اتفاقيات رسمية لمستوى الخدمة، فإنه يتعـين على الإدارة العليا التفكير في تنفيذ العمليات الرسـمية لاتفاقيات مسـتوى الخدمة المُوصى بها. حيث تسـتطيع اتفاقيات مسـتوى الخدمة أن تخلـق بيئة جديدة كلياً داخل تقنية المعلومات. ولتتمكن جميع الأطراف من فهم مسؤولياتهم والتزاماتهم تجاه الخدمة

على نحو أفضل. هذا بالإضافة إلى اعتماد اتفاقية مستوى الخدمة أساساً لتسوية العديد من المسائل.

يجب على المهنيين الذين يسعون إلى توسيع مدى إدراكهم لإدارة خدمات تقنية المعلومات أن يستخدموا المصادر الخاصة بمنتدى إدارة خدمات تقنية المعلومات itSMF الذي تم الحديث عنه سابقاً. تعتبر هذه المنظمة غير الربحية لاعباً بارزاً في عمليات التطوير والتعزيز المستمر لمعايير أفضل الممارسات الخاصة بإدارة خدمات تقنية المعلومات. ويستطيع المسئول التنفيذي المهتم بتعلم المزيد أن يزور الموقع www.itsmfi.org للحصول على المزيد من المعلومات. وسوف تقود عملية البحث إلى مواقع وطنية مستقلة لكل دولة. فهي منظمة تقبل عضويات ولكن يستطيع المرء التسجيل للدخول بصفة ضيف والوصول إلى العديد من الوثائق والأوراق والمعلومات المتعلقة بالمؤتمرات والندوات القادمة. يهتم منتدى إدارة خدمات تقنية المعلومات itSMF بالترويج لأفضل ممارسات إدارة خدمات تقنية المعلومات الخاصة بمكتبة البنية التحتية لتقنية المعلومات آيتل كما أن له اهتماماً قوياً بمعايير أيزو ٢٠٠٠٠ (ISO 20000).

معايير المجموعة المفتوحة للامتثال والأخلاقيات OCEG:

إن المجموعة المفتوحة للامتثال والأخلاقيات OCEG عبارة عن منظمة صناعية غير ربحية تعمل على تطوير المعايير وتساعد المؤسسات في تحسين عمليات الحوكمة وإدارة المخاطر والامتثال الخاصة بها. ومن خلال الدعم الكبير المقدم لها من قبل صناعة التقنية، قامت هذه المنظمة بنشر العديد من "المعايير" مثل نموذج قدرة الحوكمة وإدارة المخاطر والامتثال GRC. قمنا بوضع كلمة معايير بين علامتي اقتباس نظراً لأن المجموعة المفتوحة للامتثال والأخلاقيات لا تمتلك صلاحية وضع المعايير كما هو موجود في معايير الجمعية الأمريكية للمحاسبين القانونيين AICPA أو حتى في بعض المواد الإرشادية الخاصة بالمنظمة الدولية للمعايير ISO التي تناولنا الحديث عنها في الفصل السابع من هذا الكتاب.

يعرض هذا القسم "الكتاب الأحمر" "Red Book" الخاص بالمجموعة المفتوحة للامتثال والأخلاقيات OCEG ونموذج قدرة الحوكمة وإدارة المخاطر والامتثال GRC الخاص بها. إن هذه المواد الإرشادية للمجموعة المفتوحة للامتثال والأخلاقيات تشبه إلى حد كبير المعلومات

الإرشـادية الأخرى للحوكمة وإدارة المخاطر والامتثال وإطار حوكمة تقنية المعلومات التي يمكن العثور عليها في فصول أخرى من هذا الكتاب، ولكن مع اختلاف طفيف في التركيز أو النهج المتبع. إن اسـتخدام المجموعة المفتوحـة للامتثال والأخلاقيات لكلمة "المفتوحة" له معنى خاص بالنسبة لتقنية المعلومات، إذ يتبادل النظام المفتوح التغذية الراجعة مع البيئة الخارجية لكي يقوم بإجراء تحليل مستمر لتلك الردود وإعادة ضبط النظم الداخلية حسب الحاجـة لتحقيق أهداف النظام، ومـن ثم نقل هذه المعلومـات الضرورية مرة أخرى إلى تلك البيئـة الخارجية. وتختلف النظم المغلقة عن النظم المفتوحة بأن لها حدوداً محكمة تسـمح بتبادل معلومات طفيفة مع الخارج. تبـدو بعض المنظمات غالباً - مثل المنظمات البيروقراطية والاحتكارية ونظم تقنية المعلومات الكاسدة والتي قامت بغلق الحدود - غير صحية. فالمصطلح الشـائع بالنسـبة للعديد من نظم تقنية المعلومات الحديثة والمتطورة هـذه الأيام، هو مصطلح "المفتوحة" وهي الكلمة المناسـبة لنموذج قدرة الحوكمة وإدارة المخاطر والامتثال.

توجد الإرشادات الخاصة بالحوكمة وإدارة المخاطر والامتثال والصادرة عن المجموعة المفتوحة للامتثال والأخلاقيات في وثيقة أطلق عليها اسم "الكتاب الأحمر" الخاص بنموذج القـدرة، وتوجد هذه الوثيقة في الموقع www.oceg.org. وللعلم فإن الوثيقة الرسـمية في نسـختها الثانية حتى وقت نشر هذا الكتاب، متاحة عبر شـبكة الإنترنت، في حين أن النسخة المحسـنة متاحة فقط للأعضاء المشتركين. تحتوي نسخة الإنترنت الأساسية على وصف كامـل لنموذج الحوكمـة وإدارة المخاطر والامتثال. لكن يمكـن بتكلفة إضافية الحصول على النسـخة المحسـنة مع قوالب وغيرها من الوسائل المسـاعدة والمفيدة في تطبيق هذه الأداة. يستند نموذج القدرة هذا على مفهوم سُمي بالأداء القائم على مبادئ (Principled Performance)، وهـو نهج متكامل للحوكمـة وإدارة المخاطر والامتثال سنتحدث عنه في الأقسام اللاحقة.

تمثل صورة عناصر قـدرة الحوكمة وإدارة المخاطر والامتثال الموضحة بالشـكل (١٧-٢) قلب نموذج المجموعة المفتوحة للامتثال والأخلاقيات؛ إذ إن العديد من المفاهيم هنا تشـبه إلى حد كبير مفاهيم الحوكمة وإدارة المخاطر والامتثال التي تحدثنا عنها في فصول أخرى من

هذا الكتاب، إلا أن نموذج المجموعة المفتوحة للامتثال والأخلاقيات له نظرة صناعية ومرتكزة على تقنية المعلومات بشــكل أكــبر. إن أهداف المجموعة المفتوحــة للامتثال والأخلاقيات الخاصة بهذا النموذج يجب أن تساعد المؤسسات على عمل ما يلي:

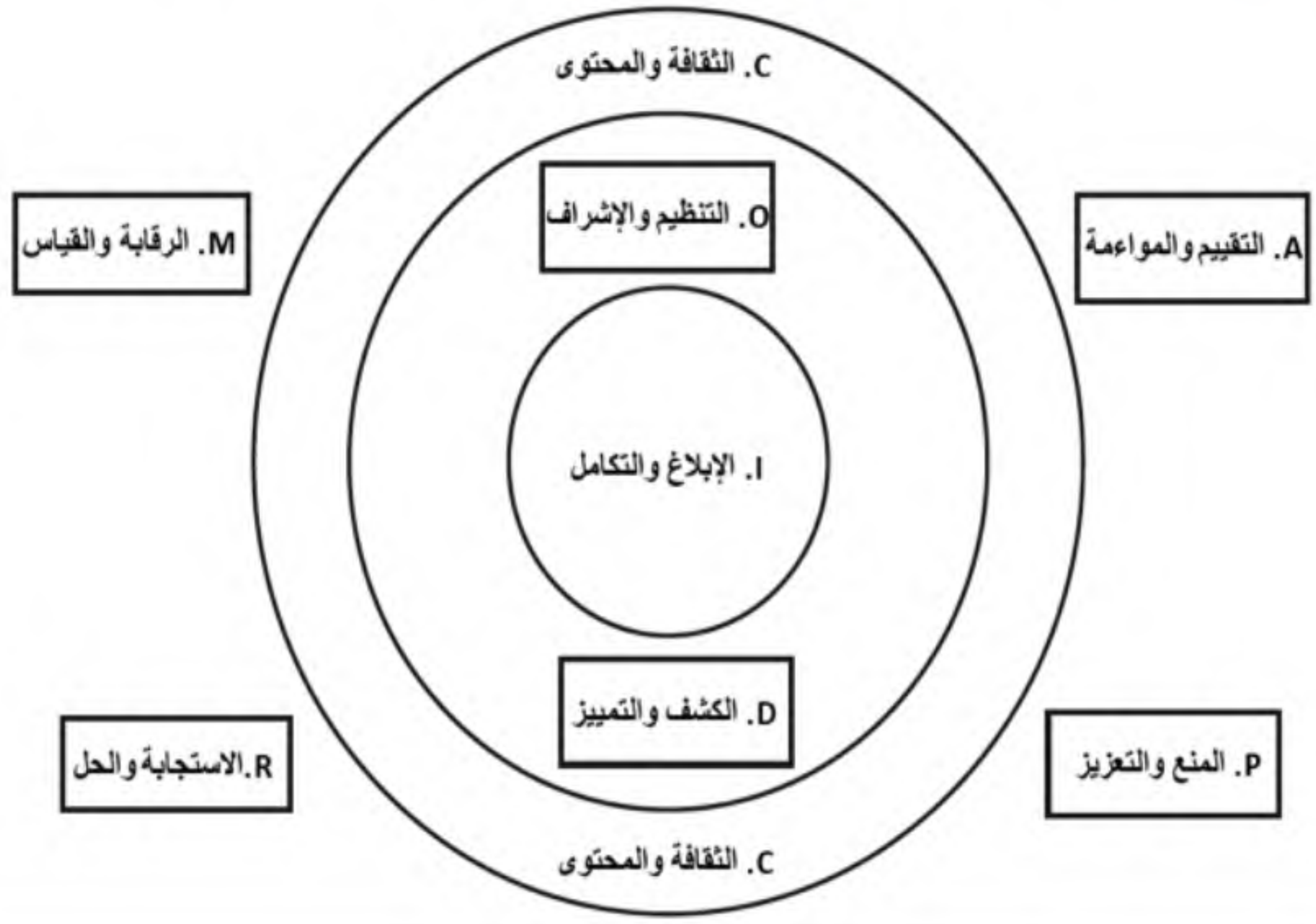
- تعزيز أهداف العمل.
- تعزيز ثقافة المنظمة.
- زيادة ثقة أصحاب المصلحة.
- تجهيز المؤسسة وحمايتها.
- منع وقوع الكوارث، والكشف عنها، وتقليصها.
- التحفيز والحث على السلوك المرغوب فيه.
- تحسين المسؤولية والكفاءة.
- تحسين القيمة الاقتصادية والاجتماعية.

مفهــوم الأداء القائــم عــلى مبادئ الخــاص بالمجموعــة المفتوحــة للامتثال والأخلاقيات OCEG:

لقد جعلــت المجموعة المفتوحة للامتثال والأخلاقيات مــن مصطلح الأداء القائم على مبــادئ علامة تجارية خاصة بهــا. حيث يصف هذا المصطلح الحاجة إلى صياغة الأهداف المالية وغير المالية للمؤسسة اللازمة لتحقيق جميع الأهداف التي تختارها المؤسسة للأخذ بها أثناء توظيف النهج الذي يتســم بالفاعلية والكفاءة والاســتجابة لدعم أهداف كل من الحوكمة وإدارة المخاطر والامتثال. الفكرة هنا هي أن جميع المؤسســات يجب أن تعمل ضمــن حدود داخلية وخارجية محددة، حيث تقوم القوى الخارجية كالمتطلبات القانونية والتنظيمية بإقامة الحدود الخارجية المفروضة. فالهدف هنا هو العمل على تكامل مبادئ وأهــداف الحوكمة وإدارة المخاطر والامتثال لمســاعدة المؤسســة على التحكم بالأداء على نحو أفضل.

شكل توضيحي (١٧-٢)

عناصر نموذج قدرة الحوكمة وإدارة المخاطر والامتثال GRC الخاصة بالمجموعة المفتوحة للامتثال والأخلاقيات OCEG



لكي تحقق المؤسسة مفهوم الأداء القائم على مبادئ Principled Performance الخاص بالمجموعة المفتوحة للامتثال والأخلاقيات، فإنه يجب عليها أن تحدد بوضوح رسالتها ورؤيتها وقيمها وأن تحدد أيضاً الأهداف التي تسعى لتحقيقها. كما يجب أن تحدد المؤسسة أيضاً كيف ستحقق أهدافها في الوقت الذي تتعامل فيه أيضاً مع المخاطر والإشكالات وحماية وخلق القيمة وتحديد فرص جديدة، والبقاء ضمن حدود معينة من السلوك الأخلاقي. كما يجب على المؤسسة أن تتحرى الشفافية في هذه الخيارات بالنسبة لأصحاب المصالح الداخليين والخارجيين، ويجب أن تحاول تحقيق جميع هذه الأمور باستخدام نهج متكامل لتحقيق أعلى مستوى ممكن من الأداء.

إن هذه المفاهيم للأداء المبدئي هي العناصر الرئيسـية لنمـوذج قدرة الحوكمة وإدارة المخاطـر والامتثال الخاصة بالمجموعـة المفتوحة للامتثال والأخلاقيـات كما هو موضح في الشكل التوضيحي (١٧-٢) والتي تم إعادة صياغتها من المواد الخاصة بالمجموعة المفتوحة للامتثال والأخلاقيات. الأقسام التالية تصف عناصر هذا النموذج بمزيد من التفصيل. يوجز هـذا النموذج مجموعة كبـيرة من المواد والمفاهيم الرفيعة المسـتوى التي تعتبر جزءاً من نموذج المجموعة المفتوحة للامتثال والأخلاقيات. نشـجع القارئ المهتم بالوصول إلى كامل النموذج من خلال عنوان الويب المشار إليه سابقاً.

عناصر القدرة والبيئة والثقافة الخاصة بالحوكمة وإدارة المخاطر والامتثال GRC:

يعرض الشـكل التوضيحي (١٧-٢) كلاً من القدرة والبيئـة والثقافة على أنها عوامل أو عناصر في نموذج الحوكمة وإدارة المخاطر والامتثال الخاص بالمؤسسـة. يهدف هذا الشكل إلى توضيح البيئة الداخلية والخارجية للأعمال والثقافة الحالية التي تعمل فيها المؤسسـة. على سـبيل المثال، يمكن لنظام الحوكمة وإدارة المخاطر والامتثال أن يعالج الأوضاع الراهنة وأن يحدد الفرص المتاحة للتكيف مع البيئة والثقافة لتحديد قيم المؤسسة من أجل تحقيق النتائج المرجوة بشكل أفضل. وباستخدام الحرف C نجد أن هناك أربعة عناصر خاصة بهذا المقطع من نموذج GRC المنشور وهي:

C1 سياق أو بيئة الأعمال الخارجية.

C2 سياق أو بيئة الأعمال الداخلية.

C3 الثقافة.

C4 القيم والأهداف.

يُعَـرِّف نموذج قـدرة الحوكمة وإدارة المخاطـر والامتثال أيضاً مجموعـة من العناصر الفرعيـة لكل عنصر من هذه العناصر. على سـبيل المثال، يحتـوي النموذج على العناصر الفرعية التالية للعنصر C3:

C3.1 تحليل الثقافة الأخلاقية.

C3.2 تحليل القيادة الأخلاقية.

C3.3 تحليل ثقافة المخاطر.

C3.4 تحليل إشراك مجلس الإدارة.

C3.5 تحليل ثقافة الحوكمة ونمط الإدارة.

C3.6 تحليل مشاركة القوى العاملة.

وكل عنصر مــن هذه العناصر الفرعيــة مدعوم بعناصر أكثر تفصيلاً لتوســيع الصورة. إضافــة إلى ذلك، يحتــوي النموذج على مجموعة مــن المبادئ وقائمة بمصــادر الإخفاقات الشــائعة لكل مبدأ من هذه المبادئ، هذا بالإضافة إلى احتوائه أيضاً على إرشادات ومراجع لمواد دعم إضافية.

عناصر القدرة والتنظيم والإشراف الخاصة بالحوكمة وإدارة المخاطر والامتثال GRC:

إن هدف الإرشــادات الخاصــة بـالمجموعة المفتوحة للامتثــال والأخلاقيات هو تنظيم ووصــف نظام الحوكمة وإدارة المخاطر والامتثال الذي يتكامل مع عمليات الأعمال القائمة والــذي يمكن أن يعدل فيها أيضاً عند الضرورة. أمــا تلك المجموعة من العناصر التي تمت الإشارة إليها بالحرف O في نموذج المجموعة المفتوحة للامتثال والأخلاقيات فهي تحتوي على العناصر الأساسية والفرعية التالية:

O1 النتائج والالتزام:

O1.1 تحديد نطاق نظام GRC.

O1.2 تحديد أنماط وأهداف نظام GRC.

O1.3 الحصول على الالتزام بنظام GRC.

O2 الأدوار والمسؤوليات:

O2.1 تحديد وتمكين قواعد الرقابة والمساءلة لنظام GRC.

O2.2 تحديد وتمكين أدوار ومسؤوليات الإدارة.

O2.3 تحديد وتمكين الأدوار والمسؤوليات القيادية.

O2.4 تحديد وتمكين القواعد التشغيلية لنظام GRC.

O2.5 تحديد وتمكين أدوار الضمان والمساءلة (مثل الرقابة الداخلية).

مــن خلال مخطط كهذا من النقــاط الفرعية والنقاط المتفرعة منها، فإنه يوجد تفصيل كاف ليســاعد المؤسســة على تأســيس وتنظيم وحــدة أو إدارة للحوكمــة وإدارة المخاطر والامتثــال. فهناك مجموعة جيدة من المبادئ ومصــادر الإخفاقات الخاصة بكل من هذه المبادئ للمساعدة في تنظيم عملية فعالة في الحوكمة وإدارة المخاطر والامتثال في المؤسسة.

إن هدف هذا الفصل هو تسليط الضوء على أن نموذج القدرة للحوكمة وإدارة المخاطر والامتثال الخاص بالمجموعــة المفتوحة للامتثال والأخلاقيات (OCEG GRC) يحتوي على بعض الأدوات الرائعة لمســاعدة المؤسسة على تأسيس إدارة فعالة للحوكمة وإدارة المخاطر والامتثال وتحســين عمليات حوكمة تقنية المعلومات. فنحن هنا نســلط الضوء فقط على بعض الخصائص الرفيعة المســتوى في هذا النموذج. فكل عنصر من هذه العناصر مدعوم بمزيد من التفاصيل.

لسنا هنا بصدد التوسع في الحديث عن نموذج المجموعة المفتوحة للامتثال والأخلاقيات OCEG والتعليــق على كل عنــصر من عناصره. بل نقوم فقط بتســليط الضوء على هذا النمــوذج للمجموعة المفتوحة للامتثال والأخلاقيات OCEG الذي يقدم بعض الإرشــادات الرائعــة لمراعاة بعض العناصر الهامة من أجل إيجاد أو وضع عمليات هامة لحوكمة تقنية المعلومات.

عناصر أخرى للمجموعة المفتوحة للامتثال والأخلاقيات OCEG:

بالتأمل في الشــكل التوضيحي (١٧-٢)، ســنرى أن كل قســم من أقســام هذا النموذج يحتوي على أهداف محددة خاصة به. على سبيل المثال، الهدف الإرشادي المعلن للقسم A من نموذج المجموعة المفتوحة للامتثال والأخلاقيات المســمى بالتقييم والمواءمة، هو تعزيز

الملف الخاص بالمخاطر في المنظمة من خلال محفظة من المخاطر والأساليب والأنشطة في هذا المجال. وتتضمن الإجراءات هنا تحديد المخاطر وتحليلها وتحسينها. على سبيل المثال، الهدف من تحديد المخاطر في النموذج المنشور هو "تحديد الأحداث والقوى والعوامل التي يمكن أن تؤثر في تحقيق أهداف الأعمال، متضمنة تلك التي تنشأ نتيجة عدم الامتثال للمتطلبات الموضوعة بمقتضى القانون أو المعايير أو السياسات الداخلية أو غيرها من الحدود."

بالتأمل في نموذج القدرة، وبالنظر إلى القسم P المسمى بالمنع والتعزيز. حيث يهدف هذا القسم إلى تشجيع وتحفيز السلوكيات المرغوب فيها ومنع الأحداث والأنشطة غير المرغوب فيها، وذلك باستخدام مزيج من الضوابط والحوافز. يحتوي هذا القسم على سبعة عناصر منها مدونات قواعد السلوك والضوابط الوقائية وعلاقات وحاجات أصحاب المصالح.

سنسلط الضوء على عنصر آخر في نموذج قدرة الحوكمة وإدارة المخاطر والامتثال GRC ألا وهو القسم R المسمى بالاستجابة والحل. ويهدف هذا العنصر إلى الاستجابة للأحداث التي تنشأ نتيجة لعدم الامتثال والأحداث غير الأخلاقية أو إخفاقات نظام الحوكمة وإدارة المخاطر والامتثال. وذلك لتتمكن المؤسسة من حل كل قضية من القضايا العاجلة ومنع وحل القضايا المشابهة مستقبلاً بكفاءة وفاعلية أكبر. ويتكون هذا العنصر من خمسة مكونات:

R1 المراجعة والفحص الداخلي.

R2 الاستفسارات والتحقيقات الخاصة بالطرف الثالث.

R3 الضوابط التصحيحية.

R4 الاستجابة للأزمات والاستمرارية والتعافي.

R5 علاج نظام الحوكمة وإدارة المخاطر والامتثال GRC.

إن العديد من هذه الإجراءات يذهب إلى ما هو أبعد من خطوات حوكمة تقنية المعلومات التي تم وصفها في فصول أخرى من هذا الكتاب الخاصة بالتحقيق في المخالفات المتعلقة بالممارسات الأخلاقية وممارسات الامتثال الخاصة بالمؤسسة. على سبيل المثال،

بالنسبة للعنصر الفرعي R1 الذي يتناول موضوع المراجعات الداخلية، فإن التوجيه هو المراجعة والجاهزية للتحقيق في المزاعم والمؤشرات الدالة على سوء السلوك أو على إخفاقات في نظام الحوكمة وإدارة المخاطر والامتثال للوقوف على الحقائق والظروف المحيطة والأسباب الرئيسية وإيجاد الحلول المناسبة لها. القاعدة هنا هي أنه لا ينبغي لمجلس الإدارة والإدارة العليا أن يكونوا أبداً هم الطرف المصدوم، بل يجب أن يكونوا على دراية بأي قضية قد تؤثر بشكل كبير في المؤسسة حين وقوعها.

يدعو المعيار المؤسسة إلى وضع إجراءات وفريق عمل أساسي للتحقيق والبحث أكثر في الشكاوى أو في التقارير الخاصة بقضايا الامتثال والقضايا الأخلاقية، وكذلك القضايا التي تم الكشف عنها أثناء عمليات الرقابة المستمرة أو التقييم الدوري لنظام الحوكمة وإدارة المخاطر والامتثال. يستمر المعيار في الدعوة إلى وضع إجراءات قوية لوضع أمور معينة في بؤرة اهتمام الإدارة العليا أو مجلس الإدارة. كما يدعو أحد المعايير التوجيهية الأخرى المؤسسة إلى أن تقوم بمراجعة أي حوادث أو بيانات مُبلغ بها بشكل دوري، وذلك لتحديد التوجهات، أو مواطن المشاكل، أو الضوابط التي بحاجة إلى تنقيح. وعليه فإن الإجراءات المقترحة أقوى مما كنا نتوقع أن نجده في العديد من المؤسسات هذه الأيام.

وبمزيد من البحث في العناصر الست الرئيسية للحوكمة وإدارة المخاطر والامتثال، نجد أن عنصر المتابعة والقياس يقع في الركن العلوي الأيسر من الشكل. حيث يحتوي هذا العنصر على الإرشادات الخاصة بإسناد المسئوليات الإدارية، وسلطة صنع القرار، والمساءلة من أجل تحقيق أهداف النظام. ويستخدم هذا العنصر الحرف M ويتكون من عناصر لمراقبة وتقييم أداء برامج الحوكمة وإدارة المخاطر والامتثال والبدء بإجراء التحسينات على النظم إذا اقتضت الضرورة ذلك.

يقر هذا العنصر بأن نظام الحوكمة وإدارة المخاطر والامتثال لابد أن يكون مرناً بما فيه الكفاية للاستجابة السريعة للتغيرات الداخلية والخارجية التي تحدث في البيئة التي يعمل بها. وأن هذا النظام سيكون أكثر فاعلية في حال كانت المؤسسة تقوم بتحديد وتقييم التغيرات المتوقعة في الوقت المناسب لتخطيط التعديلات على النظم. كما يقر النموذج أيضاً بأن الفشل في الاستجابة لأي تغيرات ضرورية في السياق قد ينتج عنه فشل في معايير

حوكمة تقنية المعلومات وفي الضوابط الحساسة لنظام الحوكمة وإدارة المخاطر والامتثال.

يدعو المعيار المؤسسة أن تقوم باستمرار بمراقبة التغيرات الداخلية والخارجية التي يمكن أن يكون لها تأثير مباشر أو غير مباشر أو تراكمي على المؤسسة. على سبيل المثال، قد تشمل التغيرات في المتطلبات الخارجية ما يلي:

- القوانين والقواعد واللوائح.
- التوجيهات والقرارات الإدارية.
- الأحكام القضائية الهامة.
- الإرشادات التنظيمية والادعائية.
- أنشطة متابعة الأوامر وفرضها.
- التزامات الجمعيات التجارية ومنظمات المعايير.

تشـير هذه القائمة إلى تحديات خاصة بالمؤسسة - خاصة الكبيرة منها وذات الجنسيات المتعـددة - والتي سـوف تواجهها عنـد محاولتها القيـام بمراقبة أحداث مثـل القرارات الحكوميـة. في أغلب الأحيان يكون الأمر أكبر من أن يتم إسـناد هـذه المهمة الرقابية إلى مجموعة واحدة للقيام بهذه المهمة الرقابية، وذلك بسبب اتساع وتنوع المعلومات. لذلك لابـد من وجود عمليات معمـول بها تحفز الإدارة على اختلاف مسـتوياتها ومواقعها على إرسـال تقاريـر بمجالات التحذير المحتملـة إلى مجموعة الإدارة المركزيـة للحوكمة وإدارة المخاطر والامتثال للقيام بمزيد من التحقيقات وتخطيط الإجراءات.

القسم I أو الإبلاغ والتكامل هو آخر عنصر في نموذج الحوكمة وإدارة المخاطر والامتثال. وهو يقع في وسـط النموذج الموضح في الشـكل التوضيحي (١٧-٢) وهدفه العام يتمثل في الحصول على المعلومات الخاصة بنظام الحوكمة وإدارة المخاطر والامتثال وتوثيقها، وإدارتها لكي يتدفق بكفاءة أعلى وأسـفل وعبر المؤسسـة الممتدة من أصحـاب المصلحة الخارجيين وإليهـم. وهذا يدعو المؤسسـة إلى تطوير وتطبيق مجموعة كبـيرة من العمليات الخاصة بمعلومات نظام الحوكمة وإدارة المخاطر والامتثال كعمليات تصنيف المعلومات، والحصول عليها، وتخزينها، وإبلاغها. وعلى الرغم من أنه ليس من الضروري أن يكون لدى المؤسسـة

نظام واحد في كل موقع، فإنه يجب أن تتناغم هذه العمليات من حيث تصنيفاتها وأشكالها وقدراتها على الاتصال.

إن بنيــة مجموعــة نظم الدعم الخاصــة بالحوكمة وإدارة المخاطــر والامتثال يمكن أن تكون أحد العوامل الرئيســية لنجاح نظــام معلومات الحوكمــة وإدارة المخاطر والامتثال بالكامــل، لكنها أيضــاً يمكن أن تكون أحد التحديات الرئيســية لتحقيق النجاح. على غرار مبــادئ COSO ERM التــي تحدثنا عنهــا في الفصل الثامن من هــذا الكتاب، فإنه يتعين عــلى المؤسســة أن تحصل على كمية كبيرة من البيانات والمعلومــات المختلفة والعمل على تصنيفها، كما يجب أن يكون لديها القدرة أيضاً على الحصول على تلك المواد لتحليلها والرد على الاستفسارات الواردة.

نمــوذج المجموعة المفتوحــة للامتثال والأخلاقيــات OCEG وحوكمة تقنية المعلومات:

إننــا لم نصل بعــد إلى النقطة التي عندهــا يمكن للمديرين ذوي الاختصاص اســتخدام محــرك البحث جوجل في البحث عن "نظم مراقبة الامتثال لنموذج الحوكمة وإدارة المخاطر والامتثال GRC الصادر عن المجموعة المفتوحة للامتثال والأخلاقيات OCEG" للحصول على قائمــة بالباعة المناســبين الذين يعرضون برمجيات نظم مراقبــة الامتثال الخاصة بـ OCEG GRC نتيجــة لعملية البحث. يوجد العديد من الأســاليب للحلول إلا أن هناك القليل من الحلول الفردية الواضحة. أحد مجالات الحلول المحتملة يمكن أن نجدها في نظم السجلات الإلكترونيــة الطبية في المستشــفيات Electronic Medical Record Systems (EMRS). ويتم تسجيل كل نشاط من الأنشطة الخاصة بالمريض، بدءاً من نتيجة الفحوصات المعملية، إلى ملاحظــات الطبيــب، إلى الأدويــة الموصوفــة، والكثير غيرها على نظــام EMRS بغرض اســترجاعها فيما بعد من أجل الاســتخدام الحالي لها أو لأغراض الأرشــفة. يجب أن يحتوي نظــام المعلومات الفعال لنموذج قدرة الحوكمة وإدارة المخاطــر والامتثال على العديد من هذه العناصر.

لقد أوجزت الأقســام السابقة العديد من عناصر نموذج القدرة للحوكمة وإدارة المخاطر والامتثال الصادر عن المجموعة المفتوحة للامتثال والأخلاقيات OCEG GRC على مستوى

عــالٍ للغايــة. إلا أن هناك نماذج أخرى تدعو إلى اتبــاع نهج أكثر تفصيلاً وفي بعض الأحيان يكــون أكثر اعتــماداً على الضوابط الإدارية. في جميع الأحوال فإن وصفنا الرفيع المســتوى هنــا للموضوع لا يقدم دراســة كاملة بالشــكل الذي يمكن أن نجــده في ٢٤٠-صفحة من المنشور الخاص بالمجموعة المفتوحة للامتثال والأخلاقيات OCEG، وفي شكله الأساسي، مع المزيد من التفاصيل في وثيقة موســعة، مما يشــجع القارئ المهتم للقيام بالمزيد من البحث والتحقيق في نموذج OCEG GRC.

إن زيــارة موقع الويب الخــاص بالمجموعــة المفتوحة للامتثال والأخلاقيات سيســمح بالوصول غير المحدود إلى مجموعة متنوعة من المواد، بعضها للاطلاع والبعض الآخر مخصص للمشــتركين. وهي المواد ذات الأهمية الخاصة مثل الكتــاب الأحمر وهو عبارة عن وثيقة تقييم لدعم إرشــادات نموذج القــدرة الخاص بالمجموعة المفتوحــة للامتثال والأخلاقيات. والغــرض منه تزويد المختصين في مجال الحوكمــة وإدارة المخاطر والامتثال بمجموعة عامة من الإجراءات المســتخدمة في التقييم والتي تتفق مع نموذج قدرة الحوكمة وإدارة المخاطر والامتثال الموضح سابقاً، وكذلك إرشادات حول ما يمكن توقعه خلال عملية تقييم أي نظام للحوكمــة وإدارة المخاطر والامتثال، مع مجموعة من الأهداف التي تســاعد المؤسســة في تقييم فاعلية تصميم وتشــغيل نظام الحوكمة وإدارة المخاطر والامتثال الخاص بها، وكذلك خفض تكلفة تلك التقييمات من خلال تقديم إجراءات محددة. كما يهدف هذا المنشــور إلى رفع مستوى نضج وجودة العمليات الخاصة بالحوكمة وإدارة المخاطر والامتثال الخاص بالمؤسسة، وذلك من خلال تقديم المساعدة في وضع خطط تحسين محددة الأولوية وتوفير مصدر خارجي للحكم والاعتراف بهذه الممارسات.

مستوى ونطاق سلطة وضع المعايير للمجموعة المفتوحة للامتثال والأخلاقيات OCEG:

كما أكدنا سابقاً، فإن المجموعة المفتوحة للامتثال والأخلاقيات لا تمتلك حتى الآن سلطة وضع المعايير كما هو حال المنظمات الأخرى مثل PCAOB والأيزو ISO. هذا بالإضافة إلى أنه بالرغم من إصدارها للعديد من المواد الإرشــادية القوية، فإن هذه المواد لا تزال تفتقر للقبول والاعتراف العالي المســتوى من قبل الآخرين حتى الآن. ومع كل هذا، فإننا نشــعر بأن أهمية المجموعة المفتوحة للامتثال والأخلاقيات والمواد الإرشادية الخاصة بها ستنمو في

السـنوات القليلة القادمة نظراً لنمو الاهتـمام بالعمليات الفعالة للحوكمة وإدارة المخاطر والامتثال وزيادة الحاجة إليها.

إن إحدى نقـاط القوة الرئيسـية للمجموعة المفتوحة للامتثـال والأخلاقيات هي أنها منظمة تطوعية بالكامل تُدار من قبل أعضاء من المنظمات الراعية وقد تم تشكيل مجلس إدارة لها من هؤلاء الأعضاء. وتضم قائمة الرعاة كبرى شركات المحاسـبة العامة مثل برايس ووترهاوس-كوبرس Pricewaterhouse-Coopers وجرانت ثرونتون Grant Thornton. هـذا بالإضافـة إلى العديد من الرعاة الرئيسـيين من قادة صناعة تقنيـة المعلومات أمثال أوراكل Oracle وسـاب SAP وكذلـك رعاة الصناعة الأمريكيـة في المقام الأول من شركات مثل عون Aon وهي إحدى الشركات الكبرى للتأمين ومتاجر التجزئة وول مارت Walmart. فإذا كان هناك أي قلق أو خوف، فمن الواضح بأنه سـيكون متوقفاً على المنظمات الراعية وأعضـاء اللجنـة الخاصة بالمجموعة OCEG. فهذه المجموعة ليسـت أكثر من أن مقرها الولايات المتحدة وليسـت منظمة دولية بالمعنـى الحقيقي. وفي عالمنا المفتوح هذه الأيام، نحن بحاجة إلى المزيد من التركيز على المواصفات العالمية.

قيمة تقنية المعلومات VAL IT: تحسين قيمة استثمارات تقنية المعلومات:

وُجِدَت جميع المؤسسـات سـواء كانت كبيرة أو صغيرة لتقدم قيمة للمسـتفيدين من خدماتهـا. وتواجه هذه المؤسسـات تحدياً حرجاً وحساسـاً فيما يخـص ضمان تحقيقهم للقيمـة من اسـتثماراتها المعقدة والمتزايدة بدرجة كبيرة في مـوارد تقنية المعلومات. وقد قام معهد حوكمة تقنية المعلومات IT Governance Institute (ITGI) الذي تم تقديمه للمرة الأولى في الفصل الخامس من هذا الكتاب، بإصدار مجموعة من المواد المتعلقة بأفضل الممارسات التي أطلق عليها اسم «قيمة تقنية المعلومات»[1] Val IT لمساعدة المؤسسة على علاج هذا التحدي وتحقيق قيمة من تلك الاستثمارات القائمة على تقنية المعلومات.

تحاول Val IT أن تعالج المشاكل المتعلقة بإدارة وحوكمة تقنية المعلومات التي تواجهها الإدارة على اختلاف مسـتوياتها. حيث إن تقنيات وممارسـات تقنية المعلومات دائمة التغير والتكيف تبعاً لممارسات الأعمال الجديدة. فكثيراً ما تستثمر المؤسسات في النظم والإجراءات الجديـدة والمنقحـة مع قليل من التخطيـط والبحث الإضافي، حيث سرعان ما تكتشـف أن

هذه المبادرات الجديدة لا تعمل كما هو مأمول أو أنها تحتاج إلى استثمار حجمه أكبر بكثير مما هو متوقع. إننا نواجه هذا الموقف كثيراً على سبيل المثال، عندما يصاب المدير المالي التنفيذي بالإحباط جراء بعض القصور في النظم المالية الخاصة بالمؤسسة. فيقوم هو شخصياً بالبحث عن أفضل الحلول الممكنة في العروض التجارية المقدمة من الموردين، ثم يعمل على تشجيع إدارة تقنية المعلومات على تبني واعتماد هذا الحل. وفي ظل هذا الضغط من أحد أعضاء الإدارة العليا ولكن بقليل من البحث والتحقيق التفصيلي فيما يخص هذا الشأن، فإن المؤسسات في بعض الأحيان تبادر في استثمارات جديدة في تقنية المعلومات بتكاليف باهظة دون الحصول قيمة حقيقية من تلك الاستثمارات. يعدVal IT أحد أطر العمل التي تحتوي على أفضل الممارسات للحوكمة، وهذا يتفق إلى حد كبير مع إطار أهداف ضوابط المعلومات والتقنيات ذات الصلة (كوبت) والذي تم الحديث عنه في الفصل الخامس من هذا الكتاب. يتكون إطار العمل كوبت من مجموعة من المبادئ الإرشادية وعدد من العمليات المُوصى بها والمرتبطة بتقنية المعلومات والتي تتفق مع هذه المبادئ والممارسات الرئيسية في الإدارة. في حين يشكل الإطار Val IT مجموعة كاملة من الأنشطة البحثية والمطبوعات والخدمات الإضافية التي تدعم الإطار الرئيسي لقيمة تقنية المعلومات Val IT كما هو موضح في الشكل التوضيحي (١٧-٣). وعلى الرغم من أن الإطار كوبت يحدد ممارسات جيدة "للوسائل" التي تسهم في عملية خلق القيمة، فإن الإطار Val IT يحدد ممارسات جيدة لتحقيق "الغايات"، وذلك من خلال تزويد المؤسسات بالهيكل الذي تحتاج إليه لقياس ومراقبة وتحسين عملية تحقيق قيمة الأعمال من استثماراتها في مجال تقنية المعلومات.

إن العديد من المؤسسات هذه الأيام بغض النظر عن حجمها وإيراداتها وصناعاتها وموقعها وأنشطة أعمالها، تقوم باستثمارات واسعة النطاق في مجال نظم تقنية المعلومات وموارد تقنية المعلومات المرتبطة بها. ومع ذلك، وفي حالات كثيرة جداً، فإنه وببساطة لا يتم تحقيق تلك القيمة لتقنية المعلومات. على سبيل المثال، في عام ٢٠٠٧ أوضحت الدراسة التي أجرتها شركة جارتنر Gartner المتخصصة في أبحاث تقنية المعلومات أن ٢٠٪ من إجمالي النفقات في تقنية المعلومات قد تم إهدارها[٢]. وهذه النتيجة توضح أن إجمالي الهدر على الصعيد العالمي نحو ٦٠٠ مليار دولار أمريكي سنوياً. وفي دراسة مشابهة أجرتها شركة جولدمان ساكس Goldman Sachs عام ٢٠٠٩ على عدد من المديرين التنفيذيين

للمعلومــات CIOs والمصنفين بأنهم أكبر ١٠٠٠ مدير تنفيــذي للمعلومات، وجدت أن ما يقرب من ٤٠٪، في المتوسط من إجمالي النفقات في مجال تقنية المعلومات لا عائد منها على المؤسســة[٣]. النقطة الرئيســية هنا هي أن العديد من المؤسسات لا تقوم بقياس أو تقييم قيمة اســتثماراتها الجارية في مجال تقنية المعلومات. وهذا يعد خســارة كبيرة من منظور حوكمة تقنية المعلومات.

شكل توضيحي (١٧-٣)

إطار عمل قيمة تقنية المعلومات Val IT



تقدم المواد[٤] الخاصة بالإطار Val IT الصادر عن معهد حوكمة تقنية المعلومات ITGI إرشــادات خاصة بتقييم القيمة المكتسبة من اســتثمارات تقنية المعلومات. إن إيجاد قيم معتمدة على تقنية المعلومات، فضلاً عن أنها ليســت بالأمر السهل، فإن معظم المؤسسات يظهر عليها واحد أو أكثر من الأعراض التالية التي تم تلخيصها واقتباسها من المواد المنشورة والخاصة بإرشادات الإطار Val IT.

- **مشــاكل في تقديــم القدرات التقنيــة:** إن إدارات تقنيــة المعلومات لــدى العديد من المؤسسات ليســت على مســتوى كافٍ من النضج لتقوم بتقديم القدرات التقنية اللازمة لدعم العمليات التشــغيلية للأعمال ولتمكين تغير الأعــمال على نحو كاف وفعال. وهذا التحدي يسلط الضوء على ضرورة تحسين عمليات حوكمة وإدارة تقنية المعلومات إما قبل أو بالتزامن مع تقديم ممارسات إدارة القيمة.

- **محدوديــة أو عدم معرفــة نفقات تقنية المعلومات:** في كثير مــن الأحيان نجد أن كبار المديرين في المؤسســة يفتقرون للرؤيــة الواضحة الكافية فيما يتعلــق بالنفقات الخاصة بتقنية المعلومات، وكذلك الاستثمارات في مجال تمكين تقنية المعلومات في جميع الخدمات والأصــول وغيرها من موارد تقنيــة المعلومات لديهم. ونجد في أغلــب الأحيان أن صناع القرار يمكنهم فقط توقع حجم الإنفاق على الاستثمارات الخاصة بتقنية المعلومات وحجم الفائدة التي ستعود عليهم جراء هذا الإنفاق وما يمكن أن تكون عليه الجدوى الاقتصادية الكاملــة جــراء هذا الالتزام. ويتــم تمويل النفقات غالباً من ميزانيات غير منســقة. مما يــؤدي إلى ازدواجية وتضارب كبيرين في عملية طلب الموارد. هذا بالإضافة إلى أنه في كثير من الأحيان نجد أن الإدارة لا تركز على قضايا حســاب التكاليف والتسعير الخاصة بتقنية المعلومات في مراجعاتها الخاصة بوضع ميزانيات تطبيقات تقنية المعلومات.

- **تنازل الأعمال عن عملية صنع القرار لصالح إدارة تقنية المعلومات:** عندما تكون الأدوار والمسؤوليات والمساءلات المتعلقة بإدارة تقنية المعلومات في المؤسسة غير واضحة، عندها ســتقوم إدارات تقنية المعلومات بانتزاع مقعد القيادة، وتحديد الاســتثمارات المطلوبة في مجــال الأعمال المعتمدة على تقنية المعلومات التي يجب البــدء بها، إذ إنها تقوم بوضع أولويات لتلك الاســتثمارات من وجهة نظرها المحدودة، مما يؤدي بشــكل غير صحيح إلى تجريد الأعمال من مسئولياتها في تحديد الجدوى الاقتصادية والدفاع عنها والتي تستخدم لتبرير كل قرار من القرارات المتعلقة بالاستثمار في مجال تمكين تكنولوجيا المعلومات.

- **ضعف التواصل بين إدارات تقنية المعلومات والأعمال:** يعتبر التعاون الوثيق بين إدارات تشــغيل تقنية المعلومات وإدارات الأعمال الأخرى بمثابة القضية الحاسمة في عملية خلق القيمة المكتســبة من تقنية المعلومات. فعند غياب مثل هذه الشراكة، ســيتأثر التواصل،

وتتزايد أوجه القصور، ويظهر الفشــل في أوجه التوافق في النشــاط، وتأخذ ثقافة التنصل وإلقاء التهم واللوم في الانتشــار داخل بيئة العمل. في بعض الحالات نجد أن إدارة تقنية المعلومات تتحول كثيراً إلى دور التابع بدلاً من دور المبتكر. كما يتم إشراكها في الاقتراحات الخاصة بالاستثمارات في وقت متأخر جداً عن عملية اتخاذ القرار لدرجة لا تستطيع معها أن تســهم في هذه الاســتثمارات بقيمة كبيرة. وفي حالات أخرى يتم إلقاء اللوم على إدارة تقنيــة المعلومات لعدم تقديمها لقيمة من الاســتثمارات الخاصة بتمكين تقنية المعلومات - وهــي القيمة التي لا يمكــن تحقيقها إلا من خلال الشراكة بــين إدارة تقنية المعلومات وإدارات الأعمال الأخرى.

- **التشــكيك في قيمة تقنية المعلومات:** مما يثير الســخرية ، أنه على الرغم من اســتمرار المؤسســات في الاســتثمار أكــثر وأكثر في الموارد التقنيــة، فإن العديد من كبار المســؤولين التنفيذيين يتســاءلون كثيراً حول ما إذا كانت القيمة المناسبة من هذه الاستثمارات قد تم تحقيقها بالفعل أم لا. حيث يكون التركيز الأكبر غالباً على إدارة التكاليف الخاصة بتقنية المعلومــات بدلاً من فهم وإدارة ومحاولة الاســتفادة من الدور الــذي تلعبه إدارة تقنية المعلومات في عملية خلق قيمة ملموســة من الأعمال. فعندما تنطوي اســتثمارات تقنية المعلومات على تغيرات تنظيمية كبيرة وبشــكل متزايد، فإن الفشــل في تحويل التركيز من التكلفة إلى القيمة سيظل مستمراً ليكون هو العائق الأكبر أمام تحقيق القيمة المرجوة من هذه الاستثمارات المتعلقة بتقنية المعلومات.

- **إخفاقــات كبيرة في الاســتثمارات:** عندما تتعثر مشــاريع تقنية المعلومــات، فقد تكون تكاليف الأعمال المرتبطة بها هائلة ومرئية بشــكل ملحوظ. حيث يمكن أن تؤدي عملية إلغاء المشاريع إلى آثار غير متوقعة ومكلفة جداً في الأعمال كما أن التجاوزات التي تحدث في الميزانيــة المخصصــة يمكن أن تؤدي إلى حرمان المشــاريع الأخرى مــن الموارد الحيوية الخاصة بها. وفي كثير من الأحيان يتم تجاهل هذه المشاكل حتى تصل إلى حد يكون فيه الوقت متأخراً لاتخاذ أي إجراء تصحيحي.

يمكن مشــاهدة هذه الأعراض في العديد من إدارات تقنية المعلومات المؤسســية. ففي كثير من الأحيان نجد أن إدارة تقنية المعلومات تقود شركاءها في الأعمال من خلال الطلبات

الخاصة بوضع أولويات وطرح خدمات جديدة دون النظر إلى قيمتها الإجمالية التي ستعود على المؤسسة جراء تلك النفقات. لذا يجب أن تعمل مواد الإطار Val IT على تشجيع جميع المشاركين على أخذ نظرة أعمق على القيمة العائدة من استثمارات تقنية المعلومات وخدماتها. وربما الأهم من ذلك هو أن يعطي الإطار Val IT الفرصة لكبار المديرين للتركيز على المجالات المتعلقة بتحقيق قيمة أكبر من العمليات الخاصة بحوكمة عمليات تشغيل تقنية المعلومات.

إطلاق مبادرة لإدارة القيمة المكتسبة من تقنية المعلومات:

تم تصميم المواد الخاصة بإطار العمل Val IT الصادر عن معهد حوكمة تقنية المعلومات ITGI لتوفير الإرشادات لإدارات تقنية المعلومات في المؤسسة والإدارة العليا التي تقوم بتمويل موارد تقنية المعلومات وجميع أصحاب المصالح المستفيدين من تلك الأنشطة الخاصة بتقنية المعلومات. من ناحية أخرى، ونظراً لأن هذه الإرشادات الخاصة بأفضل الممارسات تنشر من قبل أحد المصادر ذات الصلة بجمعية ضبط نظم المعلومات وتدقيقها ISACA (وليس على سبيل المثال في أحد مطبوعات عضو مجلس إدارة في مؤسسة)، فإن هذه الإرشادات لم تلقَ الاهتمام اللازم والكافي من قبل الإدارة العليا. ومع ذلك يعد الإطار Val IT أحد مجموعات المواد الرائعة اللازمة لدعم حوكمة تقنية المعلومات ودعم عمليات تحسين الضوابط الداخلية.

يجب على الإدارة العليا أن تناقش المسائل المتعلقة بالقيمة المكتسبة من تقنية المعلومات مع كل من إدارة تقنية المعلومات وإدارة عمليات التشغيل. والتفكير في إطلاق مبادرة لإدارة القيمة المكتسبة من تقنية المعلومات. إن أحد أفضل الطرق لمعرفة جاهزية المؤسسة للبدء في برنامج لإدارة القيمة المكتسبة هي مراجعة وتقييم المبادئ الخاصة بالإطار Val IT ومدى التزاماته للعمل على تنفيذها. وتتضمن هذه المبادئ ما يلي:

- يجب أن تُدار استثمارات تقنية المعلومات كمحافظ استثمارية. كما وضحنا في الفصل الرابع عشر من هذا الكتاب.
- يجب أن تتضمن استثمارات تقنية المعلومات النطاق الكامل للأنشطة اللازمة لتحقيق القيمة المكتسبة للأعمال من هذه الاستثمارات.

- يجب إدارة اســتثمارات تقنية المعلومــات من خلال دورات الحيــاة الاقتصادية الكاملة الخاصة بها.
- ينبغــي أن تعي جميع الممارســات الخاصة بتقديم القيمة في جميع أنحاء المؤسســة بأن هناك فئات مختلفة من الاســتثمارات، ومن ثم فإنه يتم تقييم وإدارة تلك الاســتثمارات بطرق مختلفة.
- يجب على ممارســات تقديم القيمة أن تحدد وتراقب المقاييس الرئيســية، وأن تستجيب بشكل سريع لأي تغيرات أو انحرافات.
- يجب على ممارســات تقديم القيمة إشراك جميع أصحاب المصالح في المســؤولية المناسبة وتقديــم القــدرات وتحقيق الفوائــد الخاصة بالأعــمال في ظل وجود المراقبــة والتقييم وعمليات التحسين المستمرة.

إن مديــري تقنية المعلومات وكبار المديرين المعنيين بعمليات تقنية المعلومات الخاصة بالمؤسسة- أو يجب أن يكونوا - هم المعنيين بشكل مباشر بالإشراف على الممارسات الخاصة بإدارة القيمة أو تنفيذها. فاستناداً إلى المواد الخاصة بإطار Val IT، لا بد من عقد لقاء ما بين مديري تقنية المعلومات ومديري الأعمال في المؤسسة لتقييم مدى استعدادهم للانتقال نحو إدارة قيمة تقنية المعلومات. ويقدم الشــكل التوضيحي (١٧-٤) مجموعة من الأسئلة والتأكيدات لمدى اســتعداد إدارة تقنية المعلومات لتقييم جاهزية المؤسســة للانتقال نحو إدارة تلك القيمة المتمثلة في تقنية المعلومات.

يتعــين على إدارة تقنية المعلومات التأمل في هذه الأســئلة والنقاط الموضحة بالشــكل التوضيحي (١٧-٤) فيما إذا كانت المؤسسة وفريق إدارة عمليات التشغيل على علم بأهمية إدارة القيمة المكتسبة وأنهم قاموا باتخاذ الخطوات اللازمة نحو تطبيق هذا المفهوم. بكل تأكيد فإن جميع الأطراف - إدارة تقنية المعلومات وإدارة عمليات التشــغيل - بحاجة إلى إقناعهم بأهمية إدارة القيمة المكتسبة من تقنية المعلومات.

شكل توضيحي (١٧-٤)

تقييم الجاهزية لإدارة القيمة المكتسبة من تقنية المعلومات

١. هل جميع اســتثمارات تقنية المعلومات ســواء كانت تطبيقات أم شــبكات أو الاتصالات الخاصة بالخوادم، تدار كمحفظة استثمارية؟
٢. هل تتم إدارة جميع استثمارات تقنية المعلومات لتشمل النطاق الكامل للأنشطة المطلوبة لتحقيق أهداف الأعمال المرجوة من تلك الاستثمارات؟
٣. هــل تدار اســتثمارات تقنية المعلومات من خلال دورات الحيــاة الاقتصادية الكاملة الخاصة بها، ابتداء من تكاليف إطلاق الاســتثمار أو شرائه مروراً بتكاليف التشــغيل الاعتيادية وصولاً إلى نهاية الاستثمارات؟
٤. هــل تــدرك تقنية المعلومــات والإدارة بأنه يجب أن يكون هناك فئات مختلفة من الاســتثمارات المتعلقة بتقديم القيمة، حيث يجب أن تتم إدارتها وتقييمها بشكل مختلف؟
٥. هل لدى عملية تقديم القيمة مقاييس رئيسية تم تحديدها لمتابعة أي تغيرات أو انحرافات والرد عليها بشكل سريع؟
٦. هل يبدو على الممارســات الموضوعة لتقديم القيمة المكتســبة أنها تقوم بإشراك أصحاب المصالح وإسناد المساءلة المناسبة لتقديم القدرات وتحقيق المنافع والفوائد الخاصة بالأعمال؟
٧. هل هناك عمليات متابعة وتحســين مســتمرة ومعمول بها على جميع الممارسات الخاصة بتقديم القيمة؟

تدعو الإرشــادات المنشورة والخاصة بإدارة القيمة المؤسســة إلى أن تشارك بشكل أكبر في أفضل الممارســات الخاصة بإدارة القيمة. فهي تدعو المؤسسات وأصحاب المصالح ممن لديهــم رؤية مبدئية فيــما يخص إدارة القيمة إلى تطوير الفهــم والوعي والالتزام بالمبادئ والممارســات الخاصة بإدارة القيمة. واســتناداً إلى هذا التقييم المبدئي، يمكن البدء بتحليل أكــثر تفصيلاً ونضجــاً معتمداً على المجالات الخاصة بإطار قيمــة تقنية المعلومات Val IT فيما يتعلق بحوكمة القيمة المكتســبة وإدارة المحافظ وإدارة الاســتثمارات الخاصة بتقنية المعلومات.

الشروع في إدارة القيمة المكتسبة:

تعتبر المفاهيم الخاصة بإطار Val IT هامة بالنسبة للحوكمة الفعالة لتقنية المعلومات. ومن الطرق الفعالة للبدء في عملية إدارة القيمة المكتسبة تقييم الجاهزية الحالية من خلال استخدام أسئلة تقييم الجاهزية الموضحة في الشكل التوضيحي (١٧-٤). وبمجرد إتمام هذا التقييم، فإن النتائج ستقدم لنا الأساس اللازم لتحديد المطلوب إضافته من الحالة الحالية لإدارة القيمة المكتسبة إلى الحالة المستقبلية لها، ووضع أوليات لما يجب تطويره.

استناداً إلى المواد المنشورة الخاصة بإطار العمل Val IT والصادرة عن معهد حوكمة تقنية المعلومات ITGI، فإن الخطوات الخمس التالية تلخص كيف يمكن تطبيق إطار Val IT وإدارة القيمة المكتسبة في المؤسسة. وقد تكون الاختلافات بين المؤسسات كبيرة، لذلك فإن المواد الإرشادية الخاصة بإطار Val IT تصف فقط عدداً محدوداً من نقاط البدء.

خطوة (١): بناء الوعي والفهم لإدارة القيمة: نجد في العديد من المؤسسات أن صناع القرار وأصحاب المصالح الرئيسيين لا يقدرون أهمية خلق القيمة المكتسبة أو الحاجة إليها كما يجب. فهذا المفهوم الخاص بالقيمة المكتسبة لا يظهر بشكل طبيعي من خلال خطط وأنشطة الأعمال الاعتيادية فحسب؛ بل يلزم أن يتشكل بفاعلية. ولعل المشكلة هنا تظهر في أنه على الرغم من أن مفاهيم إدارة القيمة المكتسبة موجودةٌ منذ عقود، فإن فكرة إيجاد القيمة والحفاظ عليها من خلال تغيير الأعمال في المؤسسات الحديثة يكون التعامل معها عادة على أنها مبدأ ضمني.

بالنسبة للعديد من المؤسسات لا يوجد هناك فهم موحد ومشترك لما يمكن أن يشكل قيمة للمؤسسة، وما مستوى العمل والجهد المطلوب لتحقيق تلك القيمة أو كيف يمكن قياس تلك القيمة. مما كان له بالغ الأثر في العديد من المؤسسات، وضياع أو فشل تنفيذ العديد من الفرص التي كان من شأنها إيجاد القيمة، مما أدى إلى تآكل مفهوم القيمة أو تدميره.

إن مديري العمليات التشغيلية والمديرين الماليين ومديري تقنية المعلومات في المؤسسة بحاجة إلى إيجاد قاعدة واسعة من الوعي بضرورة الحاجة إلى إدارة القيمة وتنشئة الوعي بما هو مطلوب لتطوير هذه القدرة، متضمناً ذلك التزامات داخلية قوية خاصة بالإدارة والسلطة التنفيذية لتحسين إيجاد القيمة والإبقاء عليها بمرور الوقت.

في ظل الفهم القوي لإدارة القيمة، يجب أن تتغير السلوكيات التنظيمية والفردية لإلقاء نظرة أوســع على مستوى المؤسســة بالكامل واتباع نهج أكثر انضباطاً واعتماداً على القيمة لصنــع القرار. كل هذا من شــأنه أن يؤدي إلى الإدراك والقبــول المتزايد لضرورة أن تعمل إدارات تقنيــة المعلومات مع غيرها مــن إدارات الأعمال معاً في إطار من الشراكة المدعومة بأدوار، ومســئوليات ومســاءلات واضحة تتعلق بإدارة القيمة، مما يقودنا إلى تحقيق قيمة أكبر من الاستثمارات الخاصة بتمكين تقنية المعلومات.

خطوة (٢): تطبيق حوكمة قوية لتقنية المعلومات: إن العمليات والأدوار والمسؤوليات والمســاءلات المرتبطة بتحقيق القيمة المكتســبة من الاســتثمارات الخاصــة بتمكين تقنية المعلومــات بحاجة إلى تحديد وقبول بشــكل واضح. ففي كثير مــن الأحيان تكون الأدوار والمســؤوليات والمســاءلات الخاصة بتقنية المعلومات غير واضحة إذا ما قورنت بغيرها من إدارات الأعمال. في بعض الأحيان يتم صنع القرارات المرتبطة بالأعمال من قبل إدارة تقنية المعلومات، في حين أن القرارات المرتبطة بتقنية المعلومات يتم صنعها من قبل الأعمال. في بيئــة كهذه تكــون ثقافة اللوم والتنصل وإلقاء التهم هي الســائدة، وذلك في ظل الالتباس المستمر فيما يخص المساءلة والمسؤولية والرعاية.

تحتــاج المؤسســة إلى وضع إطار عمــل خاص بحوكمــة تقنية المعلومــات مع تحديد واضــح للأدوار والمســؤوليات والمســاءلات. وينبغي أن يكون هذا الإطــار مدعوماً بقيادة قوية وملتزمة، وعمليات مناســبة، وهياكل ومعلومات تنظيمية، ونظام مكافآت ملائم. في ظــل إطار لحوكمة المعلومات مثل هذا يجب أن تنمو التوجهات والســلوكيات التنظيمية، والفردية نحو رؤى أعمق وأكثر إســتراتيجية للمؤسسة. لذا يتعين على المسؤولين التنفيذيين ومديري تقنية المعلومات وعمليات التشــغيل أن يعتمدوا نهجاً أكثر انضباطاً واعتماداً على القيمــة المكتســبة في اتخاذ قراراتهم ومســاءلاتهم. ففي ظل وجود حوكمــة قوية لتقنية المعلومــات، ينبغــي أن تؤدي البيئة الأكثر كفاءة في صنع القرار إلى رفع مســتوى الثقة بين إدارة تقنية المعلومات وباقي إدارات الأعمال الأخرى. وســتكون النتيجة تحقيق قيمة أكبر من الاستثمارات الخاصة بتمكين تقنية المعلومات.

خطوة (٣): إجراء جرد لاستثمارات تقنية المعلومات: بالنسبة للعديد من المؤسسات، هناك رؤية ضعيفة، هذا إن وجدت، فيما يتعلق بعدد ونطاق وتكلفة الاستثمارات الخاصة بتمكين تقنية المعلومات الحالية والمخطط لها أو الموارد، ســواء المخصصة للاســتثمارات أم اللازمة لدعم تلك الاســتثمارات. في كثير من الأحيان يكون إجمالى نفقات تقنية المعلومات في المؤسسة غير معلوم. وتأتي هذه النفقات غالباً من ميزانيات مختلفة وغير منسقة وبقدر كبير من الازدواجية. ففي العديد من المؤسسات يحدث عادة صراع كبير على طلب الموارد الخاصة بتقنية المعلومات.

ولحل هذه المشكلة لا بد للمؤسسة من إنشاء محافظ للاستثمارات والخدمات والأصول وغيرها من الموارد المتعلقة بتقنية المعلومات ســواء كانت مقترحة أم فعلية. وهذا المفهوم أكــبر حتى من أفضل الممارســات للإطار آيتل الخاصة بإدارة التهيئة والتي تمت مناقشــتها في الفصل الســادس من هذا الكتاب. ونتيجة لعملية إنشــاء هذه المحافظ، لا بد أن يتغير الســلوك والتوجهات التنظيمية والفردية لتشــمل الرؤية الواسعة للمؤسسة، لذا لا بد من وجود العمليات والممارسات المعمول بها لدعم ذلك.

أهــم الفوائد التي تعود من عملية جرد كهذه للاســتثمارات الخاصة بتقنية المعلومات هــي زيادة الفهم والإدراك لمعرفة ما تم إنفاقه بالضبط وعلى أية اســتثمارات تخص تقنية المعلومات، وفي أي مجال من مجالات الأعمال كانت تلك الاســتثمارات، ومن هو المســئول عنها. الفائدة الأخرى هي التحديد الأفضل للفرص لزيادة القيمة المكتسبة من خلال ضبط عملية تخصيص التمويل، والحد من التكلفة الإجمالية للمؤسسة عن طريق إزالة التكرارات، والاســتخدام الأكثر فاعلية للموارد، وتقليــل المخاطر من خلال الفهم الأفضل لتلك المحافظ الخاصة بتقنية المعلومات.

خطوة (٤): توضيح قيمة الاســتثمارات الفردية لتقنية المعلومات: بالنســبة للعديد من المؤسســات إن لم يكــن معظمها، لا توجــد عملية تطبيقية تتم بشــكل متناغم لتحديد قيمة الاســتثمارات المحتملة أو الحالية لتقنية المعلومات. إنما يمكن تحديد هذه القيمة بأنها صافي إجمالي فوائد دورة الحياة من إجمالي تكاليف دورة الحياة المهيئة للمخاطر وعلى أساس القيمة الزمنية للأموال. ونتيجة لذلك، فإن بعض أصحاب المصالح يتســاءلون باستمرار عما إذا كانت

استثمارات تقنية المعلومات قد أوجدت قيمة أم لا. تكون دراسة الجدوى الخاصة باستثمارات تمكين تقنية المعلومات غالباً غير موجودة أو سـيئة الإعداد، ويتم التعامل معها عادة من قِبل إدارة تقنية المعلومات على أنها مجرد مرجعية إدارية لازمة فقط لتأمين التمويل. يوجد القليل إن لم يكن لا شيء من معلومات ما قبل الاستثمار عن تكاليف تقنية المعلومات كما لا يوجد أي دقة في التحليل لتحديد تلك الفوائد أو القيمة. لا يوجد سوى القليل من المقاييس التي تُمكِّن من متابعة ورصد القيمة التي بصدد الإنشـاء أو التي تم إيجادها. في كثير من الأحيان نتصور أن التقنية أو إدارة تقنية المعلومات سوف تقدم قيمة سحرية.

يجـب على المؤسسـة أن تضـع عملية خاصـة بتطويـر وتحديث دراسـات الجدوى الشـاملة والمعدة بشكل ملائم فيما يتعلق بالاستثمارات الخاصة بتمكين Business Cases تقنية المعلومات، متضمناً ذلك جميع النشـاطات المطلوبة لخلق القيمة. كما يجب وضع دراسـة الجدوى باستخدام نهج من أعلى – لأسفل. بدءاً من صياغة نتائج الأعمال المرجوة بشـكل واضح واسـتكمالاً بوصف الإجراءات المطلوب إنجازها وعلى يد من ستتم. كما أن دراسـات الجدوى هذه يجب أن يتم تحديثها واستخدامها أداة تشغيلية خلال دورة الحياة الاقتصادية الكاملة الخاصة باستثمار تقنية المعلومات.

ونتيجـة لهذه العملية، فإن التوجهات والسـلوكيات التنظيمية والفردية لا بد أن تتغير لتكريس المزيد من الجهد المبذول للتخطيط لاستثمارات تقنية المعلومات وتطوير دراسات الجدوى وتحديثها بشـكل مستمر. إن من شأن التقييم الأكثر موضوعية لدراسات الجدوى الخاصة باسـتثمارات تقنية المعلومات أنه يُمكِّـن من عمل مقارنات أفضل وأكثر موضوعية بين الأنواع المختلفة من الاسـتثمارات الخاصـة بتقنية المعلومات. فهناك فرص أكبر لمقارنة الاستثمارات الفردية استناداً إلى قيمتها النسبية مقارنة بالاستثمارات الأخرى المتاحة وكذلك استناداً إلى مسار سجل Track record قوي لاختيار الأفضل. كما يجب أن يكون هناك أقل مستوى من عدم التأكد والمخاطر من أن القيمة المستهدفة لن تتحقق.

الخطـوة (٥): إجـراء تقييـمات وترتيـب أولويات واختيـارات لاسـتثمارات تقنية المعلومـات: لا يوجد حالياً أي عملية تطبيقية مسـتمرة لإجراء تقييـم موضوعي للقيمة النسـبية لجميع استثمارات تقنية المعلومات المقترحة والحالية. خاصة فيما يتعلق بتحديد

الأولويات والاختيار من بين استثمارات تقنية المعلومات ذات القيمة المحتملة الأكبر. إن العديد من القرارات الاستثمارية الخاصة بتقنية المعلومات في المؤسسة هذه الأيام غير موضوعية وتكون سياسية غالباً. فمجرد اتخاذ القرار بالمضي قدماً في استثمار ما، فمن النادر جداً إعادة النظر فيه ما لم تحدث بعض الأزمات الحرجة. إذ يتم نادراً علاج أو إلغاء استثمارات تقنية المعلومات السيئة التنفيذ في الوقت المناسب والكافي للتقليل من الخسائر. فإذا تم إلغاؤها، فإنهم ينسبون الفشل إلى شخص ما ويجب تحميله المسئولية ومحاسبته.

إن الحل الخاص بإطار العمل Val IT هو تطبيق نظم إدارة المحافظ لتصنيف استثمارات الأعمال المعتمدة على تقنية المعلومات. كما يجب على المؤسسة أن تُنشئ معايير وتقوم بتطبيقها بصرامة لدعم عمليات التقييم المتناغمة والمتجانسة للاستثمارات طوال دورة حياتها الاقتصادية بالكامل. ونتيجة لذلك، فإن التوجهات والسلوكيات التنظيمية والفردية يجب أن تتغير لتشمل النظرة الواسعة لدى المؤسسة وتبني مزيد من الشفافية.

إن الفائدة من هذا النهج المكون من الخطوات الخمس هي الفرص المتزايدة لخلق القيمة من خلال اختيار استثمارات تقنية المعلومات الأكثر احتمالاً لتقديم القيمة. ويجب أن تتبع هذه الفرصة إدارة فعالة لتلك الاستثمارات والإلغاء المبكر للاستثمارات التي يبدو أنها لن تستطيع أن تحقق القيمة المرجوة. وتقدم مواد الإطار Val IT المزيد من التفاصيل المرتبطة بتلك المنهجيات.

يقدم الإطار Val IT إرشادات مفيدة وعمليات وممارسات مجربة في حوكمة واختيار وإدارة الاستثمارات الخاصة بتمكين تقنية المعلومات. ويصف الإطار Val IT العمليات المترابطة التي من الضروري أن تكون في موضع التنفيذ إذا ما أرادت المؤسسات أن تضمن القيمة المكتسبة الأمثل من استثماراتها. لم يقم هذا القسم إلا بتسليط الضوء واستخراج بعض المواد من المواد الإرشادية الخاصة بقيمة تقنية المعلومات. إن إطار Val IT هو أحد المفاهيم الخاصة بحوكمة تقنية المعلومات، وهو مفيد للغاية في تقييم القيم النسبية لتقنية المعلومات الموجودة في عمليات إطلاق التطبيقات الجديدة لتقنية المعلومات وبناء الضوابط العامة للإدارة. الأهم من ذلك هو ضرورة وصول تلك المفاهيم الخاصة بقيمة تقنية المعلومات إلى إدارة تقنية المعلومات والإدارة العليا ليتمكنوا من فهم استثماراتهم في موارد تقنية المعلومات على نحو أفضل.

ملاحظات:

1- Val IT Framework for Business Technology Management, www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-Pages/Val-IT1.aspx?utm_source=multiple&utm_medium=multiple&utm_content=friendly&utm_campaign=va.

2- IT Financial Management, Gartner Consulting, www.gartner.com/it/products/consulting/GTACaseStudy.pdf. f

3- Independent Insight: IT Spending Survey, "2009 Under the Knife—Expect –1% Global Decline," Goldman Sachs, November 2, 2009, www.scribd.com/doc/7737986/Goldman-Sachs-IT-Spending-Survey.

4- John Thorp, "Val IT Framework 2.0—Adding Breadth and Depth to the Value Management Road Map," ISACA Journal (June 2008): 1–3.

الجزء الخامس

متابعة وقياس حوكمة إدارة المؤسسة ومجلس الإدارة

الفصل الثامن عشر
إدارة محتوى المؤسسة

يصــف مصطلــح إدارة محتوى المؤسســة ECM، وهــو أحد مصطلحــات إدارة تقنية المعلومــات التي لم تكن شــائعة حتى الســنوات الأولى مــن القرن الحالي، الإســتراتيجيات والأســاليب والأدوات المســتخدمة لحيــازة وإدارة وحفظ وتقديم المحتــوى والوثائق ذات الصلة بالعمليات التنظيمية. وقد أصبحت الآن إحدى المجموعات الخاصة بأنشــطة تقنية المعلومات التي تشــهد نمواً سريعاً، فإدارة محتوى المؤسسة عبارة عن سلسلة من العمليات التــي تغطــي إدارة المعلومات داخل نطاق المؤسســة بالكامل بغض النظــر عما إذا كانت تلك المعلومات على هيئــة وثائق ورقية أو ملفات إلكترونية أو بيانات مطبوعة من قاعدة البيانات أو رســائل البريد الإلكتروني أم بيانات مخزنة في البيئة الســحابية لتقنية المعلومات أو عــلى أي هيئة من الهيئــات العديدة الأخرى المتطورة للمعلومــات والبيانات. وتهدف عمليات إدارة محتوى المؤسســة في المقــام الأول إلى إدارة دورة حياة المعلومات ابتداءً من إنشائها مروراً بأرشفتها وحتى التخلص منها في نهاية المطاف.

تهدف إدارة المحتوى المؤسسي إلى جعل إدارة معلومات الشركات والوثائق الداعمة لها أكثر ســهولة، وذلك من خلال تبســيط تخزينها وأمنها وضبط إصداراتها وتوجيه معالجتها والقدرة على الاحتفاظ بها. إن الفوائد التي تعود على المؤسســة جراء اســتخدامها للعمليات الفعالة لإدارة المحتــوى تتضمــن كفاءات محســنة وضوابط أفضل وتكاليف أقل. على ســبيل المثال، تســتخدم معظم البنوك هذه الأيام عمليات إدارة المحتوى المؤسسي للاحتفاظ بالنسخ الورقية من الشيكات القديمة بدلاً من الطريقة القديمة لحفظ الشيكات الورقية في مستودعات ورقية ضخمة. فطبقاً للأنظمة القديمة والتقليدية، فإن طلب العميل الخاص بالحصول على نســخة من شــيك قد يستغرق عدة أســابيع، حيث كان يجب على موظفي البنك الاتصال بالمستودع لمخاطبة شــخص كان دوره تحديد موقع الصندوق والملف والشــيك المطلوبين ومن ثم يقوم بســحب الشيك وعمل نسخة منه ومن ثم إرســاله إلى البنك من خلال البريد، والذي يقوم في النهاية بإرساله إلى العميل بواسطة البريد. أما في حال وجود نظام لإدارة المحتوى المعمول به

في المؤسســة فإن موظف البنك يستطيع بكل بســاطة أن يقوم بالبحث في النظام عن حساب العميل ورقم الشــيك المطلوب. وبمجرد ظهور صورة الشــيك على شاشــة الحاسب، يستطيع الموظف إرساله فوراً إلى العميل عبر البريد الإلكتروني، وذلك أثناء انتظار العميل على الهاتف.

تســتطيع العمليات الفعالة لإدارة المحتوى المؤســسي أن تعمل عــلى خفض التكاليف وتحســين العمليــات، ســواء كانت هذه العمليات تخص الشــيكات في أحــد البنوك أو أي مجموعة متنوعة من الوثائق الورقية الأخرى. إن العمليات الفعالة لإدارة المحتوى المؤسسي تعد من الأدوات الهامة التي تســاعد في تعزيز حوكمة تقنية المعلومات في المؤسسة. يقدم هــذا الفصــل المفاهيم الخاصــة بإدارة المحتوى المؤســسي ECM ويناقــش المجالات التي يســتطيع المدير التنفيذي من خلالها تحســين جميع عمليات حوكمة تقنية المعلومات من خلال تطبيق عمليات إدارة المحتوى المؤسسي

خصائص إدارة المحتوى المؤسسي ومكوناتها الرئيسية في المؤسسة اليوم:

تشتمل العوامل التي تشجع الأعمال والشركات على تبني واعتماد الحلول الخاصة بإدارة المحتوى المؤسسي على جميع الاحتياجات اللازمة لزيادة كفاءة المعاملات الخاصة بالأعمال، وتحســين ضبط المعلومات، وخفض التكلفة الإجمالية لإدارة المعلومات بالنسبة للمؤسسة. حيث تعمل تطبيقات إدارة المحتوى في المؤسســة على تســهيل الوصول إلى الســجلات من خــلال عمليات البحث باســتخدام الكلمات الرئيســية والنص الكامل، الأمر الذي يســمح للموظفــين بالحصول على المعلومات التي يحتاجون إليهــا مباشرة من مكاتبهم خلال ثوانٍ قليلة بدلاً من البحث في تطبيقات متعددة أو استخراجها من السجلات الورقية.

تستطيع نظم إدارة محتوى المؤسسة تعزيز ضبط ومراقبة السجلات لمساعدة المؤسسات على تحســين عمليات خدمة العملاء والامتثال للوائــح الحكومية والصناعية مثل متطلبات قانون ســاربينز أوكســلي SOx، التي تمت مناقشــتها في الفصل الثاني من هــذا الكتاب أو معيــار أمن بيانات صناعة بطاقات الدفع (PCI DSS)، والذي جاء ذكره في الفصل الحادي عشر من هذا الكتاب. وتعد المهام الأمنية ســواء كانت على مســتوى المستخدم أو الإدارة، والخيــارات الأمنية الخاصة بســجلات البيانــات كذلك من المكونات الهامــة في نظام إدارة المحتوى المؤسسي وذلك لحماية البيانات الحساسة.

كما يســتطيع نظام إدارة المحتوى المؤسسي أن يقلل من الاحتياجات التخزينية والورقية والبريديــة، ويزيد من كفــاءة الموظفين، كما يؤدي أيضاً إلى قرارات مؤسســية أفضل وأكثر استنارة ووعياً، وكلها أمور من شأنها أن تقلل من التكاليف الإضافية لإدارة المعلومات. يعد نظام إدارة المحتوى المؤســسي ضرورياً وهاماً خاصة بالنسبة للمؤسسة التي لديها متطلبات لها علاقة بالاحتفاظ طويل الأجل بالمســتندات والمتطلبات الخاصة بالاحتفاظ بأحجام كبيرة من المستندات. وفي ظل احتياجاتنا لوثائق مخصصة، يمكن لنظام إدارة المحتوى أن يساعد من خلال عمليات مدعومة بالتوقيع أو إدارة أصول رقمية لوســائط غنية أو إدارة تصاميم تقنية أو ضخمة الصياغة وغير ذلك.

مــن ناحية أخرى، فــإن نظام إدارة المحتوى المؤســسي لا يعد من الأنظمــة المغلقة أو من فئة المنتجات الفريدة أو المتميزة. وتُســتخدم عبارة عمليات إدارة المحتوى المؤســسي مصطلحاً جامعاً يشــير إلى مدى واسع من التقنيات الموضوعة في المؤسسة والموردين الذين يتعاملون معها. ويعمل نظام إدارة المحتوى المؤســسي بشــكل مناســب عندما يكون "غير مرئي" بصورة فعالة بالنســبة للمســتخدمين. وتقوم تقنيات نظام إدارة المحتوى المؤســسي بدعــم تطبيقات مخصصة مثل الخدمــات الفرعية، وتكون تلك التقنيــات غالباً عبارة عن مجموعة من المكونات الخاصة بالبنية التحتية التي تناسب النماذج ذات الطبقات المتعددة وتتضمن جميع التقنيات المرتبطة بالوثائق والسجلات الموجودة في المؤسسة لمعالجة وتقديم وإدارة كل من البيانات المركبة والمعلومات غير المركبة معاً. وعلى هذا النحو، فإن عمليات نظام إدارة المحتوى المؤســسي تعد إحدى المكونات الرئيســية والضرورية في مجال تطبيق الأعمال الإلكترونية الشاملة.

عمليات إدارة المحتوى المؤسسي وحوكمة تقنية المعلومات:

تعد إدارة محتوى المؤسسة إحدى الإســتراتيجيات المستمرة والمتطورة للوصول إلى رفع مســتوى كيفية اســتخدام جميع معلومات المؤسســة إلى الدرجة القصوى. حيث تســمح أدوات وإستراتيجيات إدارة المحتوى المؤسسي للمؤسسة بإدارة كلٍّ من البيانات والمعلومات المركبة وغير المركبة الخاصة بأعمال المؤســة بصرف النظــر عن أماكن وجودها. وبالطبع فــإن القيام فقط "بــإدارة" هذا المحتوى من المعلومــات لا يُعد أمراً كافيــاً. فالقدرة على

الوصــول إلى الإصدار الصحيح لإحدى الوثائق أو السـجلات يُعدُّ مــن الأمور الهامة، ولكن يجب إدارة هذا المحتوى لكي يتم اســتخدامه بالشــكل الذي يحقق أهداف الأعمال. ومن الممكن أن تكون الأدوات والتقنيات الخاصة بإدارة المحتوى المؤســسي هنا ضرورية وهامة للقيام بإدارة كامل دورة حياة المحتوى الوثائقي منذ إنشائه وحتى التخلص منه.

إن إدارة المحتــوى المؤســسي عبارة إســتراتيجية مســتمرة ومتطورة لزيــادة الكيفية التــي يجب من خلالها اســتخدام هذا المحتوى المعلوماتي للمؤسســة والــذي قد يكونُ أساســياً لنجاح العمليات التشــغيلية لأعمال المؤسســة. وعلى الرغم مــن وجود العديد من البرمجيات والعروض الأخــرى التي يقدمها الموردون، فإنه يجب على الإدارة أن تفكر في تنفيذ واســتخدام نظام إدارة المحتوى المؤســسي من حيث مفاهيم الامتثال والتعاون والاستمرارية والتكلفة.

عــلى الرغم من حقيقة أن المؤسســات اليوم تواجه زيادات هائلة في أحجام ومســتوى تعقيد أعمالها ونظمها، فإن العديد منها لايزال يَســتخدم الطرق التقليدية القديمة نفســها القائمــة عــلى التعامل مع الوثائق واحــدة تلو الأخرى. وقد تفطن المؤسســة إلى أن بعض الكفــاءات وعمليات حوكمة تقنية المعلومات قد تتحســن من خلال اعتماد عمليات إدارة المحتوى المؤســسي للمؤسســة. وكنقطة انطلاق فإنه يتعين عــلى الإدارة أن تقوم بمراجعة دورة حياة محتوى الوثائق لديها. إن هذه الفكرة مشابهة لحديثنا عن دورات حياة تطوير النظــم (SDLCs) التي تناولها الفصل الخامس عشر من هذا الكتاب. لكن يجب أن يقوم هنا كل من فريق تقنية المعلومات والإدارة بوضع خريطة تفصيلية لمجريات تدفق أو ســير العمليــات الخاصة بالوثائق والمعلومات الحالية لمعرفــة الأماكن التي يمكن أن يجدوا فيها تداخلات، وكذلك المجال الذي يمكن من خلاله التحسين في الإستراتيجيات الخاصة بتطبيقات الأعمال وتدفق المعلومات.

تُظْهِــر المعلومات التي تم جمعها حجــم التعقيدات الكامنة في العمليات التي تتعامل مــع إدارة محتوى منظمة ما. لــذا يجب أن يكون الهدف هو بناء معمارية لإدارة المحتوى في المؤسســة. كما هو موضح في الشكل التوضيحي (١٨-١)، والذي قد يشمل العديد إن لم يكن كل من العناصر التالية:

- **استحواذ نظام إدارة المحتوى المؤسسي (ECM) على جميع الوثائق:** يجب أن تركز عمليات إدارة المحتوى المؤسسي على حفظ وتتبع واستخدام المستندات كافة، سواء كانت وثائق ورقية أم رقمية أو وثائق لوسائط غنية كالفيديو أو الشعارات أو الصور. كما يجب أن تتعامل مستودعات الوثائق مع الوثائق المهيكلة وغير المهيكلة، مع الإقرار بأن تلك الأصول الرقمية يكون لها قيمة عالية من الملكية الفكرية. ومن الممكن أن يكون مستودع الوثائق عبارة عن نظام ضخم ومعقد ويكلف مئات الآلاف من الدولارات، أو يكون نظاماً بسيطاً كنظام الملفات والمجلدات المستخدم في شركة صغيرة. والمهم أن يكون لديهم معلومات يمكن العثور عليها بمجرد أن يتم وضعها في النظام.

- **خبرة المستخدمين وأدوات التشارك:** التعاون هو فن العمل بشكل جماعي. ويعد ضرورياً بالنسبة للتقنيات المرتبطة بإدارة المحتوى المؤسسي مثل الرسائل الفوريةً وألواح الكتابة (السبورات) والاجتماعات التي تتم عبر الإنترنت، ووسائل البريد الإلكتروني التي تسمح بإتمام العمل أينما وعندما يكون هناك حاجة إليه. ويسمح التعاون لأفراد بخبرات متكاملة أو متداخلة أن يقدموا نتائج أفضل وأسرع من ذي قبل، الأمر الذي يسمح لوحدات التشغيل وفرق الأعمال بالعمل سوياً في أي وقت، سواء كانوا في مكاتب متجاورة أم منفصلين بعضهم عن بعض في أي مكان في العالم.

- **دورات حياة سير العمل:** تعد الأدوات ضرورية لنقل المحتوى طيلة الدورات المحددة لعمليات العمل، كالعمليات اللازمة لمعالجة المطالبات. ولابد من استخدام أدوات إدارة المحتوى المؤسسي في تطوير ونشر ومراقبة وتحسين عدة أنواع من التطبيقات الآلية. ويتضمن ذلك العمليات التي تشتمل على كل من النظم والناس. ترتبط دورات حياة سير الأعمال أيضاً مع العمليات اليدوية لإدارة الوثائق، كما يجب على دورات سير العمليات معالجة الموافقات وتحديد الأولويات التي يتم بناء عليها ترتيب الوثائق والمستندات التي يتم تقديمها. وفي الحالات الاستثنائية يقوم مخطط سير الأعمال بتصعيد قرارات مبنية على قواعد محددة سلفاً قد تم وضعها من قبل مالكي النظام.

- **إدارة السجلات الخاصة بنظام إدارة المحتوى المؤسسي:** في حين أن أي جزء من المحتوى يمكن تسميته سجلاً. إلا أنه يجب التعامل مع هذه العناصر وفقاً لجدول زمني للاحتفاظ

بها والذي يحدد المدة التي يتم الاحتفاظ خلالها بالسجل، ويكون ذلك بناء على اللوائح النظامية أو الممارسات التجارية الداخلية. كما أن هناك احتياجات لتخزين هذه السجلات المتعددة والمتنوعة بحيث يمكن استرجاعها عند الحاجة، وحذفها في نهاية المطاف في الأوقات المناسبة لاحقاً.

- **أدوات محتوى الويب، الوسائط الغنية:** يجب أن تقوم عمليات إدارة المحتوى المؤسسي بمعالجة العمليات الخاصة بإنشاء المحتوى ومراجعته واعتماده ونشره على شبكة الإنترنت. وتشتمل البيانات الرئيسية للمحتوى الموجود على شبكة الويب على أدوات الإنشاء والتأليف أو التكامل وإدارة وتصميم المدخلات وقالب العرض وإدارة إعادة استخدام المحتوى وقدرات النشر الفعالة.
- **أدوات التشارك في نظام إدارة المحتوى المؤسسي وأدوات الحوسبة الاجتماعية:** تُمكن التقنيات المستخدمة في التعاون أو التشارك المستخدمين المستقلين، كالموظفين أو شركاء العمل، من أن يقوموا بسهولة بتشكيل فرق المشروع والحفاظ عليها، بغض النظر عن الموقع الجغرافي. إن هذه التقنيات وأدوات الحوسبة الاجتماعية تقوم بتسهيل العمل التعاوني وإنشاء المحتوى القائم على الفريق، واتخاذ القرار لكل من نظم تقنية المعلومات التقليدية والعدد المتزايد لعمليات حوسبة الشبكة الاجتماعية في المؤسسة. كما أن هناك حاجة إلى الاحتفاظ بسجلات مناسبة لهذه الأنشطة.
- **البحث وتحليلات المحتوى:** سواء كان بسبب الإستراتيجيات التسويقية أو الوصاية الحكومية أم غيرها من العوامل، فالمؤسسات بحاجة متزايدة للقيام بمراجعة وتحليل العديد من المعاملات الخاصة بأعمالها. فعلى الرغم من أننا نمتلك قاعدة بيانات قوية كأحد أدوات المساعدة، فإن عمليات إدارة المحتوى المؤسسي يمكن أن تساعد كثيراً في الإبقاء على نتائج هذه الأنشطة.
- **أدوات الاستمرارية والاحتفاظ:** يعد الإبقاء على الأعمال سارية ومستمرة أربعاً وعشرين ساعة في اليوم، وسبعة أيام في الأسبوع ٧/٢٤، أحد مهام التخطيط للاستمرارية، ونظراً لأن الوثائق الإلكترونية هذه الأيام تعد بمثابة شريان الحياة بالنسبة لمعظم المؤسسات، فإن إدارة المحتوى المؤسسي لديها تلعب دوراً هاماً في إدارة الاستمرارية. حيث تسمح

التقنيات الخاصة بإدارة المحتوى المؤسسي بإنشاء مستودعات مركزية يمكن أن تتواجد بها كل المعلومات الحيوية للشركة. وسوف تختلف طريقة التخزين اعتماداً على مدى أهمية المحتوى بالنسبة للشركة، وهي تتنوع من أشرطة النسخ الاحتياطي خارج الموقع إلى المواقع الإضافية والمواقع الانعكاسية (المرآوية) المفصولة جغرافياً والموجودة على شبكات طاقة مختلفة. كما يجب على المؤسسة أن تضع أوليات لعناصر المحتوى لديها لتحديد مدى السرعة اللازمة لاستعادة محتوى الوثيقة على شبكة الإنترنت حال حدوث كارثة، كما يلزم تحديد العمليات المحورية في أداء المهام والكيانات التي تعتمد عليها، على أن يلي ذلك إجراء تقييم تأثير الأعمال لتحديد أثر حدوث عرقلة لتلك العمليات أو فقدها. لذا فوجود عمليات مناسبة وقوية لإدارة المحتوى المؤسسي يعد هنا من الأمور الضرورية.

- **وسائل لإشراك عملاء نظام إدارة المحتوى المؤسسي:** إن وجود الأدوات التي تسمح للمؤسسة وعملائها وغيرهم من أصحاب المصلحة باسترجاع جميع المستويات الخاصة بأنشطة التعاملات والوصول إليها بسهولة يجب أن يكون سمة رئيسية من سمات عمليات نظام إدارة المحتوى المؤسسي. هذا النوع من الأدوات يسمح لمركز خدمات العملاء بتوفير تواريخ عمليات الشراء بشكل سريع بدلاً من العودة إلى السجلات واسترجاعها.

- **إدارة الوثائق:** تساعد عمليات إدارة المحتوى المؤسسي هنا المنظمات على تحقيق إدارة أفضل للقيام بإنشاء ومراجعة واعتماد واستخدام الوثائق الإلكترونية. توفر إدارة الوثائق الميزات الرئيسية كالخدمات المكتبية وتوصيف الوثائق والبحث وتسجيل الدخول والخروج والتحكم في الإصدار وتاريخ التنقيح وأمن الوثائق.

- **روابط التشغيل البيني للمؤسسة:** تحتاج المؤسسة عادة في هذه الأيام إلى تبادل البيانات والمعلومات بين وحداتها التشغيلية المختلفة وأصحاب المصالح الخارجيين. وعلى الرغم من أن النظم والتصميمات المختلفة قد تتسبب في وجود صعوبات، فإنه ينبغي أن تكون عمليات إدارة المحتوى المؤسسي مفتوحة ومرنة بما يكفي لبناء روابط تشغيل بيني للنظم التي تغطي المؤسسة بكاملها ووحداتها التشغيلية.

- **أدوات أمــن إدارة المحتوى المؤســـسي:** يجب أن تقوم عمليات إدارة المحتوى المؤســـسي بفرض قيود على عمليات الوصول إلى المحتوى أثناء إنشائها وكذلك إدارتها عند تسليمها. وينبغي أن تشتمل هذه العمليات الأمنية على ما يلي:

- **إدارة الحقوق الرقمية:** يجب أن تقوم عمليات إدارة المحتوى المؤسسي بمنع التوزيع غير المشروع للمحتوى المحمي بالحقوق عن طريق تقييد الوصول إلى المحتوى وصولاً (نزولاً) إلى مستوى الجملة وكذلك منح / تقييد الصلاحيات للتوجيه إلى المحتوى والوصول إليه.

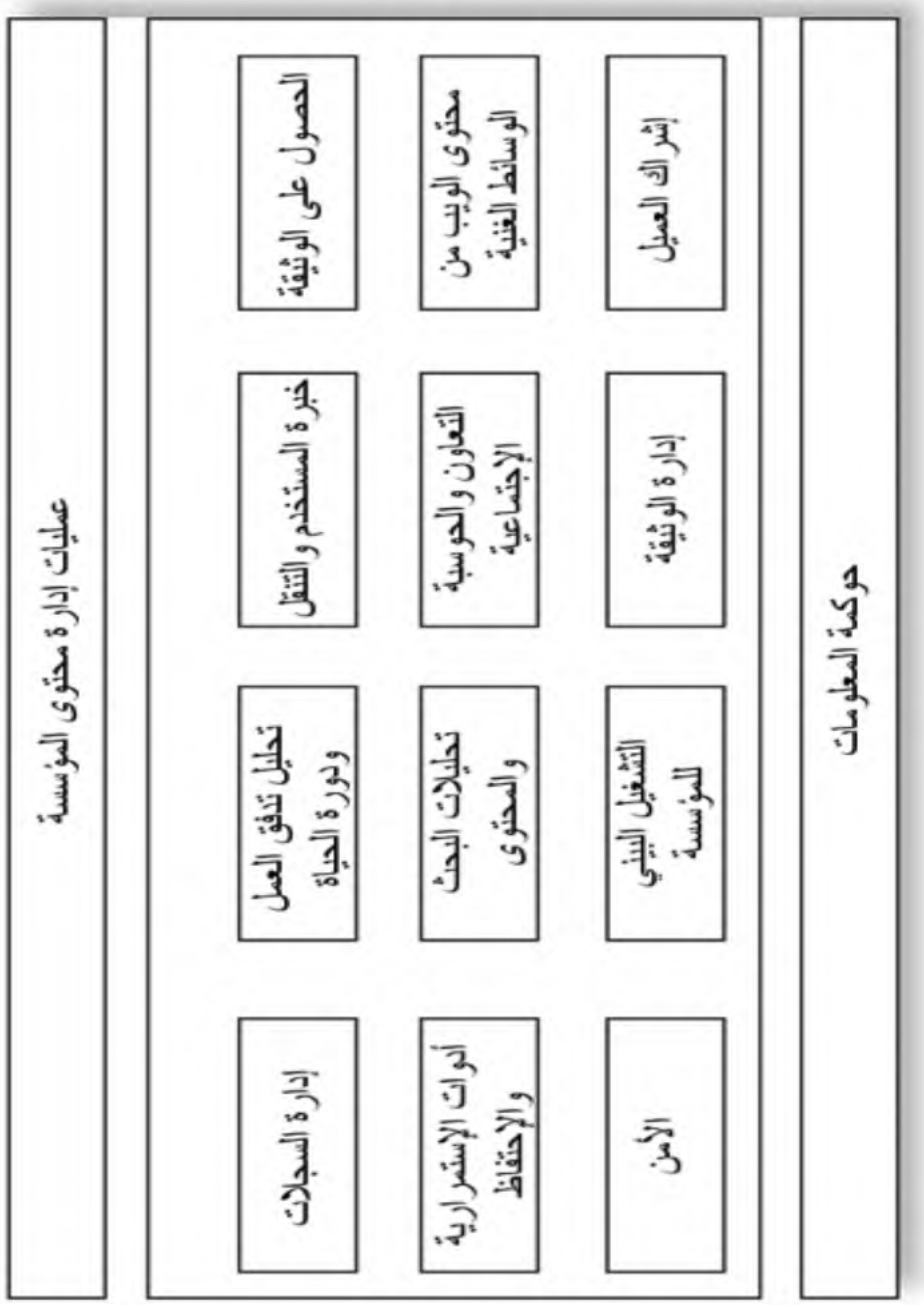
- **التوقيعات الرقمية:** يجب أن تتأكد العمليات من هوية مرسل الوثيقة وسلامة الرسائل.

هنــاك عنــصران آخران في إطار بنية نظام إدارة المحتوى المؤســـسي الموضح في الشـــكل التوضيحي (١٨-١) لا يجب تجاهلهما. فالمربع أو الجزء العلوي من هذا المخطط عبارة عن مســـاحة يطلق عليها إدارة الامتثال. فالعنصر الأساسي في إستراتيجية الامتثال الناجح لنظام إدارة المحتــوى هو الحاجة إلى الدمج بــين فكرة الامتثال لنظام إدارة المحتوى والأعمال وألا يُنظر للامتثال هنا كما لو كان مشروعاً يمكن أن يبدأ و"ينتهي"، وعلى الرغم من أن الامتثال للوائح التنظيمية يعد أمراً شــاقاً، فإنه يجب أن يُنظر إليه على أنه فرصة لتحسين العمليات المشــتركة للأعمال، وليس فقط مجرد تكلفة مســتمرة على الأعمال. إن هذا المســتوى من الامتثــال يختلــف قليلاً عن مكون الامتثــال - الحوكمة وإدارة المخاطــر والامتثال - GRC الخاص بحوكمة تقنية المعلومات.

إن التأسيس السليم للمبادرة الخاصة بالامتثال سيعود بالفائدة على العديد من مجالات الخبرة في المؤسســـة خصوصاً المجالات القانونية وتقنية المعلومات وإدارة الســجلات، والتي تهــدف جميعها إلى دعــم الأهداف العامة للأعمال المؤســسـية. ويجب أن تســهم معرفة ومرئيــات الأفراد العاملــين في كل من هذه المجالات في تحقيق الفوائد المرجوة من البرنامج الســـليم للامتثــال. وعلى الرغم مــن أن الامتثال لا يمثل دائماً مشـــكلة تقنيــة، فإن تقنية المعلومات، والنمو الهائل للمحتوى غير المركب، قد يســـهمان في كشـــف محتوى الشركات. وقد يساعد الاستخدام السليم لأدوات إدارة المحتوى المؤسسي في الحد من التكلفة الإجمالية للامتثال بالنســـبة للأعمال وفي تحسين حوكمة تقنية المعلومات بشكل عام، كما هو موضح في العنصر الموجود في أسفل الشكل التوضيحي (١٨-١).

شكل توضيحي (١٨-١)

معمارية إدارة محتوى المؤسسة ECM



خلق بيئة فعالة لنظام إدارة المحتوى المؤسسي في المؤسسة:

كما أشرنا في النقاشات التمهيدية لهذا الفصل، ليست إدارة المحتوى المؤسسي مجرد نظام واحد ولكنه أكثر من إسـتراتيجية للمؤسسـة، فهو عبارة عن سلسلة من النظم والعمليات

لإدارة العديــد من النماذج والصيغ التي تتعامل معها المؤسســة اليوم بشــكل أفضل، بدءاً من الوثائق الورقية وصولاً إلى الملاحظات المنشــورة على تويتر Twitter والرسوم الهندسية، وما هو أكثر من ذلك بكثير. وقد قامت بعض إدارات تقنية المعلومات في المؤسســة بوضع إســتراتيجية خاصة بإدارة المحتوى المؤســسي، وربما تكون قد قامت بتطبيــق ذلك النهج الخاص بتلك الإســتراتيجية إلى حد كبير. ومن الممكــن أن تكون بعض الإدارات الأخرى قد قامت بتطبيق بعض الأجزاء الفعالة في نظام إدارة المحتوى المؤســسي كنظام خدمة العملاء للتحقق من الطلبات، ولكن لا يزال لدى تلك الإدارات الوســائل التي تســلكها قبل إطلاق نظام لإدارة المحتوى المؤســسي بشكل كامل. ثم من الممكن أن يكون هناك بعض الشركات التي لم تتناول المفهوم بالشــكل الصحيح ومن ثم اســتمرت في استخدام أساليبها التقليدية القائمة على التعامل مع الوثائق واحدة تلو الأخرى.

يمكن أن تكون العمليات الفعالة لإدارة المحتوى المؤسسي وسيلة جيدة جداً لتحسين حوكمة تقنية المعلومات في المؤسسة. الشكل التوضيحي (١٨-٢) يوضح بعض الشروط التي يجب على الإدارة مراعاتها عند اعتماد إســتراتيجية خاصة بإدارة المحتوى المؤسسي. فإذا قامت المؤسسة بتحقيق واحد أو أكثر من تلك المتطلبات، ولاسيما إذا قامت بتلبية العديد منها بشكل مناسب، فمن الممكن أن تستفيد من عملية تحولها لاستخدام نظام إدارة المحتوى المؤسسي.

يتطلب التحول إلى استخدام نظام إدارة المحتوى المؤسسي شكلاً من أشكال الإستراتيجية في خطــوة أولى. حيــث تتضمن بعــض الخيارات الخاصــة بوضع إســتراتيجية للتحول إلى استخدام نظام إدارة المحتوى المؤسسي على مستوى المؤسسة ما يلي:

- القيام بداية ببناء منصة جديدة لإدارة المحتوى المؤسسي في أماكن العمل، وذلك باستخدام إحدى العروض المقدمة من مقدمي خدمات المنصات الفردية لإدارة المحتوى المؤسسي.
- تهجير واســتبدال جميع نظم إدارة المحتوى الموجــود إلى منتج واحد جديد خاص بإدارة المحتوى والذي حصلنا عليه من قِبل أحد الموردين الذي يعمل على مستوى المؤسسة.
- نقــل أو تحويــل كل نظم إدارة المحتــوى الموجودة إلى المنتج الفــردي الموجود الذي تم اختياره لإدارة المحتوى على مستوى المؤسسة والمقدم من قبل البائع.

شكل توضيحي (١٨-٢)

متطلبات المؤسسة التي تبرر الانتقال إلى نظام إدارة المحتوى المؤسسي

- الاحتفاظ الطويل الأجل بالسجلات أو المتطلبات.
- الاحتياجات اللوجستية لإدارة السجلات المادية واسترجاعها.
- الاحتياجات الخاصة بامتلاك المعلومات أو السجلات كبيرة الحجم.
- احتياجات التوافق مع معايير إدارة السجلات (على سبيل المثال، الحكومة الاتحادية أو الأيزو).
- البيئة اللازمة لمشروع إدارة ومعالجة القضايا والحالات.
- عمليات السجل أو المستند المهمة المدعومة بالتوقيع.
- إدارة الأصول الرقمية (الوسائط الغنية).
- إدارة التصميمات التقنية أو الضخمة الصياغة.
- متطلبات إدارة الأصول والمرافق.
- بوابات شبكة الإنترنت الخارجية / التي يتعامل معها العملاء.
- الحاجة للتعامل مع شريك خارجي لتقديم حماية الجدران النارية.
- تطبيقات لإدارة عمليات المهام الصعبة.
- المتطلبات أو الاحتياجات اللازمة لإدارة الطباعة / الإخراج / الإحالات.
- التكامل الوثيق مع نظم ERP / CRM / LOB.
- اتصالات النظم الواردة ذات القنوات المتعددة.
- متطلبات إدارة الحقوق الرقمية/ للأصول ذات القيمة العالية.
- متطلبات تشفير البيانات التي على درجة عالية من الأمن.

- التعديل أو الاستبدال أو التحويل الانتقائي للعديد من النظم الإدارية/ المحلية المعمول بها حالياً حسب الحاجة.
- تركيب نظم إدارية جديدة متخصصة حسب الحاجة لتحقيق الأهداف المحلية.
- الانتقال إلى منصة نظام إدارة المحتوى المؤسسي القائمة على البيئة السحابية والمقدمة من قبل طرف ثالث.

ليس الهدف من هذا الفصل تقديم التفاصيل اللازمة لتطبيق إستراتيجية إدارة المحتوى على مستوى المؤسسة بواسطة استخدام العناصر التي تم وضعها، أو عن طريق التعامل مع أحد الباعة الرئيسيين مثل آي بي إم (IBM) أو إي إم سي (EMC) والذين بإمكانهم تقديم الإرشـادات والأدوات اللازمة. تُقدم الأجزاء التالية من هذا الفصل وصفاً للعناصر الأساسية لكامل نظام إدارة المحتوى المؤسسي أو لسلسلة من العمليات. كما يجب أن تشتمل الإدارة الفعالة للمحتوى على معظم هذه العناصر.

سمات نظام إدارة المحتوى المؤسسي: الأرشفة Archiving:

تضطر الأعمال هذه الأيام إلى التعاطي مع مجموعة كبيرة من مصادر البيانات المختلفة للشركات والإدارات. والتي تتضمن قواعد البيانات العلاقية، ومستودعات الوثائق، ومخازن البريـد الإلكتروني، وخوادم الملفات. والأمر الـذي يزيد من حجم التحدي الناجم عن إدارة هذه البيئـة المعقدة لمصادر البيانات المختلفة هو المتطلبات المتعلقة بمقتنيات وممتلكات الـشركات والتشريعات التنظيميـة وحوكمة المعلومـات والتفويضات للحـد من التكلفة التشغيلية من خلال البائع وتعزيز البنية التحتية. وتحتاج المؤسسة إلى مستودعات خاصة بأرشـفة وثائق نظام إدارة المحتوى المؤسـسي، وذلك لتخزين تلك الوثائق التي تكون غالباً ملايـين من البيانات والوثائق والصور، وغيرها مـن الوثائق التي تخص العملاء. ويجب أن يشتمل هذا الأرشيف على جميع الوثائق الفردية الخاصة بالاستكشاف والتحقق من سلامة وصحة المحتوى وتنظيم العمليات التخزينية والاسترجاع والتوزيع والتوصيل.

ترتبـط الفهارس الخاصة عادة بأرشـفة وثائـق نظام إدارة المحتوى المؤسـسي بمحتوى المسـتند عند إنشـاء ذلك المحتوى وذلك من خلال اسـتخدام محـركات التركيب، أو أثناء تحميلها في الأرشيف. تصميم الفهرس هنا مهم، فبمجرد وضع الوثائق في الأرشيف سيكون مـن الصعب جداً نمـو أو زيادة تلك الفهارس لـكي تلبي الاحتياجات المتغـيرة للأعمال أو الاحتياجات الخاصة بالعملاء طبقاً لوجهات النظر المختلفة لهم.

وعلى الرغم من أن مشروع الأرشفة الخاصة بإدارة المحتوى المؤسسي قد يكون "مشروعاً مرعباً"، فإنه يوفر فرصة لتوضيح مسائل مثل رقم الحساب ومعايير التسمية التي قد تكون فريدة داخل مؤسسة واحدة ولكن تتكرر عبر السجلات المحفوظة لدى الشركة. فبالإضافة

إلى إطلاق مجموعة من العمليات الخاصة بإدارة المحتوى المؤسسي، يمكن للأرشفة أن تعود على المؤسسة بفوائد فورية ـ وطويلة الأجل.

سمات نظام إدارة المحتوى المؤسسي: عمليات التصنيف Classification Processes:

تعمل عمليات التصنيف الخاصة بوثائق نظام إدارة المحتوى المؤسسي على أتمته تنظيم المحتويات غير المركبة، وذلك من خلال تحليل النص الكامل لوثائق ورسائل البريد الإلكتروني. ومــن خلال تصنيف المحتوى، بإمكان تقنية المعلومــات أن تقوم بتسريع عمليات الوصول إلى المحتــوى أو تقليل الوقت اللازم للوصــول إليه، وذلك للحصول على القيمة المرجوة من الاســتثمارات المتعلقة بنظام إدارة المحتوى المؤســسي كأرشــفة المحتوى أو إدارة السجلات الإلكترونية. ويجب أن تسمح عمليات التصنيف بالتالي:

- تقديم أعلى عوائد الاستثمار من العملية عن طريق تحرير المستخدمين النهائيين من عبء المهام اليدوية دون المخاطرة بتعارض المشاركة -في حين أنه يتم تصنيف كميات كبيرة من المحتوى بدقة.
- تصفية أرشــيف الوثائق من رســائل البريد الإلكــتروني والوثائــق ذات القيمة المحدودة بالنسبة للأعمال.
- تنظيم محتوى الوثائق بمنطق ثابت وموثوق به وقابل للتدقيق.
- أكــثر اســتعداداً للتكيف مع التغييرات في السياســات والفئات من خــلال دمج التغذية الراجعة للمستخدم في الوقت الحقيقي.
- إنشاء تصنيفات عالية الدقة للوثائق من خلال الجمع بين أساليب متعددة للتصنيف مثل:
    - قواعد الكلمات المفتاحية والتطابق التقريبي.
    - استخراج النمط.
    - الأساليب القائمة على السياق الدقيق للغاية الخاصة بـ"التعلم من خلال قدوة".

إن عمليــة تحليلات المحتوى هي العنصر الرئيسي في عمليات تصنيف وثائق نظام إدارة المحتوى المؤســسي، وهي عملية متقدمة للبحث والتحليلات تُمَكِّن من اتخاذ قرارات أفضل اعتــماداً على محتوى المؤسســة بغض النظر عــن مصدر ذلك المحتوى أو شــكله. بإمكان الحلول الخاصة بعملية تحليلات المحتوى فهم معنى وســياق لغة الإنســان وتقوم بسرعة بمعالجة المعلومات لتحســين البحث الذي تحركه المعرفة وإظهار رؤى جديدة من محتوى المؤسسة الخاصة بك.

ومــا هو أكثر تطوراً من ذلك اســتخدام تقنيات أحدث لمعالجــة اللغات الطبيعية مثل تقنيــة (IBM Watson DeepQA)، وذلــك عنــد إجراء عمليات تحليــل المحتوى، وهذه التقنية عبارة عن آلة متطورة تعمل بنظام الرد على الأسئلة. إن كمية كبيرة من المعلومات التي تم إنشاؤها واستخدامها من قِبل المؤسسة عبارة محتوى غير مركب، والذي ينمو عادةً بمعدل ضعف معدل البيانات المركبة. إن تســخير واســتخدام هذه المعلومات غير المركبة وشبه المركبة قد يساعد المنظمة للعمل بطريقة أذكى ويخدم العملاء بشكل أفضل ويتحكم في التكاليف ويخطط للمستقبل.

سمات نظام إدارة المحتوى المؤسسي: التخلص من الوثائق وإدارة الحوكمة:

يجــب أن تكون عملية التخلص من الوثائــق وإدارة الحوكمة جزءاً لا يتجزأ من عمليات إدارة المحتوى المؤسسي في المؤسسة. إذ تساعد هذه العملية المؤسسة على الوفاء بالتزاماتها للحصــول على المعلومــات وإدارتها على أســاس القيمة والتخلص مــن المعلومات العديمة القيمة أو الالتزامات في أقرب فرصة ممكنة. فقد تساعد العملية المُحْكَمة على التخلص من البيانات التي لم تعد مســتخدمة في الحد بشــكل كبير من حجم المعلومات ومن التكاليف الناجمة عن اســتخدام تقنية المعلومات. فمن خلال الحلول المناسبة للتخلص من البيانات وإدارة الحوكمــة يمكن لتقنية المعلومات أن تقــوم بإدارة المعلومات وفقاً لقيمة أعمالها أو التزاماتها القانونية وتقوم بالتخلص من المعلومات الأخرى.

إن العنصر الأســاسي في عمليات التخلص من الوثائق هو أنه يجب على إدارة المؤسســة وإدارة تقنية المعلومات الحصول على رؤية واضحة للوثيقة فيما يخص أنه يجب على إدارة المؤسســة وإدارة تقنية المعلومات الوصول إلى رؤيــة لكل من وثائق الالتزامات القانونية -

كالجداول القانونيـة لإدراج الوثائق والاحتفاظ بها - والقيمـة التجارية لمعلومات محددة مرتبطـة بأحـد الأصول أو بهوية أحـد الموظفين. كما يجب أن يكون لـدى عمليات إدارة المحتوى المؤسـسي أهداف للقيـام بالنقل الفوري للمتطلبات والحقائق بين كل من قسـم تقنية المعلومات والسـجلات والكادر القانوني للمؤسسـة، وذلك من خلال التبليغ التلقائي لمهام البنود والإشعارات والتنبيهات وعمليات البحث المبسطة في الالتزامات القانونية.

يجب على المنشـأة أن تقوم بالتخلص المبرر من الوثائق، وذلك من خلال إجراء عمليات دقيقة لجرد البيانات بهدف التخلص من المعلومات المخزنة الزائدة عن الحاجة. فمن خلال تمكـين تقنية المعلومات لإجراء عمليات تحديد النُسـخ المكررة البيانات نفسـها والبيانات القديمـة التي لم يعد لها أي قيمة تجاريـة أو عليها التزامات قانونية وكذلك النظم المكررة، فإنـه يمكن لعمليات إدارة المحتوى أن تُمَكِّـن الشركة من الاحتفاظ فقط بالبيانات التي لها قيمة محتملة.

وتسـتطيع العمليـات المناسـبة لإدارة المحتوى المؤسـسي أن تمنع تراكـم البيانات غير الضرورية في المسـتقبل. فعندما تقوم المؤسسـة بالتخلص المبرر من المعلومات التي يمكن الاسـتغناء عنها فإن ذلـك يمكنه أن يقضي عـلى مخاطرة ترتبط بتقنيـة المعلومات تُعرف بـ"ادخـار كل شيء"، ومن ثم زيادة الكتلة القابلة للاستكشـاف. كما أنه يحمي المؤسسـة من الانشـغال بممارسات تخلص مفرطة وغير مناسبة بسـبب إجرائها عمليات غير مناسبة وإهدارها لفترات حفظ لم تكون مطلوبة.

هناك مئات الحلول الأخرى لممارسـة إدارة الوثائق المكتبيـة مثل التصوير والتطبيقات الهندسـية وإدارة محتـوى الويب والمحتـوى القائم على XML وتطبيقـات نشر الوثائق. فـإدارة الوثائق تتيح آليات البحث والوصـول إلى الوثائق الموجودة في تلك النظم في جميع أنحاء المنظمة في الوقت الذي تتبنى فيه المعايير الصناعية التي تسـاعدها على التكامل مع عمليـات الأعمال الأخرى. وتقـوم إدارة الوثائق بزيادة حجم البنية التحتية الخاصة بنظام إدارة المحتوى المؤسـسي لتشـمل وثائق العمل التي تم إنشاؤها بشكل فردي أو عن طريق العمليات التعاونية.

هنـــاك العديد مـــن التقنيات والحلول المتاحة التي يقوم المـــورد بتوفيرها هذه الأيام في إدارة المحتـــوى المؤســـسي، إلا أن نظـــام إدارة المحتوى الأكثر أهمية هـــو الذي يمتلك خطة إســـتراتيجية مســـتمرة ومتطورة لزيادة الكيفية التي يمكن من خلالها اســـتخدام المحتوى. قـــد تكون العمليات المتعلقة بمعلومات نظام إدارة المحتوى المؤســـسي بمثابة نقطة انطلاق للمؤسســـة للقيام بمراجعة وإنشاء دورة حياة مشـــتركة لمحتوى المعلومات. وكنقطة بداية لحوكمـــة تقنية المعلومات، يجب على المؤسســـة رســـم خريطة لنظمهـــا وعملياتها الحالية لتحديد أوجه التداخل ومجالات التحسين للتطبيقات والإستراتيجيات التي تقوم بتطويرها. وقـــد تكون المعلومات المُجمَّعَة بمثابة مؤشر فقط على درجة التعقيد المتأصلة في أي عملية تدير محتوى منظمة ما. وينبغي أن تتمثل الخطوة التالية في مناسبة الأدوات التقنية لتلبية احتياجات الأعمال. ويمكن للتقنية أن تضمن انســـيابية إدارة المحتوى، لكن الإســـتراتيجية الأساسية يجب أن تأتي أولاً.

الفصل التاسع عشر
دور التدقيق الداخلي في الحوكمة

من المعلوم أن مهنة التدقيق الداخلي ليست جديدة وإنما هي موجودة منذ القدم. فقد اكتشــف علماء الآثار أن الكتبة في بلاد ما بين النهرين(*) قد اســتخدموا ســجلات محاسبية دقيقــة مــن ألواح الطين منذ ما يقرب من ٣٠٠ ســنة قبل الميلاد حيــث كانت تحتوي تلك الســجلات على مــؤشرات ونقاط وعلامات تحديد، وهو الأمر الــذي يدل على وجود وظيفة التدقيــق في ذلك الوقت. ودون شــك فقد تطورت مهنة التدقيق على مدى آلاف الســنين، ونقــوم اليــوم عادة بتصنيف معظم مدققــي الأعمال إما إلى مدققــين خارجيين أو مدققين داخليين. حيث يتم اعتماد المدقق الخارجي من قبل هيئة تنظيمية ليقوم بزيارة المؤسســة أو المنشأة لمراجعة أعمالها والقيام بإعداد تقرير مستقل بنتائج هذه المراجعة. ففي الولايات المتحدة يكون المدققون الخارجيون عادة هم المحاســبين القانونيين، الذين يحملون تراخيص من الولاية ويتبعون المعايير الخاصة بالمعهد الأمريكي للمحاســبين القانونيين (www.aicpa.org). كــما يوجد هناك أيضاً أنواع أخرى من المدققين الخارجيين الذين يعملون في مجالات مثل من يقومون بمراجعة مدى مطابقة الأجهزة الخاصة بالمعدات الطبية للمعايير أو مراجعة معدلات مشاهدي التلفاز أو غيرها من التقييمات في مجالات حكومية متعددة.

يكون مجال التدقيق الداخلي غالباً أكثر اتســاعاً وأهميــة من مجال التدقيق الخارجي. وكون المدقق الداخلي من موظفي أو أعضاء المؤسســة، فإنه يقوم وبشكل مستقل بمراجعة وتقييم العمليات التشغيلية في العديد من المجالات المختلفة، مثل إجراءات الرقابة الداخلية للمكاتــب المحاســبية أو العمليات الخاصة بالجــودة الصناعية. ويقــوم معظم المدققين الداخليين باتباع معايير رفيعة المســتوى تم وضعها من قبل المنظمة المهنية التي يتبعونها، وهــي معهد المدققين الداخليــين (IIA، www.theiia.org)، غير أنــه يوجد اليوم كثير من الممارســات والأســاليب المختلفة الأخرى في التدقيق الداخلي نتيجة لطبيعته العالمية وكثرة أنواع أنشطة التدقيق.

(*) بلاد العراق قديماً (المترجم).

يتخصص بعـض المدققين الداخليين في مراجعة الضوابط المالية الداخلية للمؤسسـات، في حـين يركز البعض الآخر على عمليات الأعمال أو المسـائل التشـغيلية. وعلى الرغم من أن جميـع المدققـين الداخليـين اليوم يجب أن يكـون لديهم بعض المعرفـة عن الضوابط الداخلية المتعلقة بتقنية المعلومات، فإن هناك أيضاً تخصصاً مهنياً قوياً يعرف باسم مدقق تقنيـة المعلومات. وقد تم الحديث عن هؤلاء المهنيين في الفصل الخامس من هذا الكتاب باعتبارهم الموارد الرئيسية لتطوير وتنفيذ عمليات قوية وفعالة لحوكمة تقنية المعلومات.

يسـتعرض هذا الفصل أهميـة التدقيق الداخـلي وتدقيق تقنيـة المعلومات في وضع عمليات فعالة لحوكمة تقنية المعلومات. وسوف نستعرض بإيجاز المعايير والأنشطة المهنية الخاصة بالتدقيق الداخلي والضرورية لإيجاد ممارسـات جيـدة لحوكمة تقنية المعلومات. وعلى الرغم من أن إدارة التدقيق الداخلي تعد إدارة منفصلة ومستقلة داخل المؤسسة، فإن التقاريرالصـادرة عنها تُقدَّم فقط للجنة التدقيق التابعة لمجلس إدارة المؤسسـة، لذا يجب على المديرين التنفيذيين فهم الأدوار المنوطة بهم والعمل معهم بهدف تحسـين العمليات الخاصة بحوكمة تقنية المعلومات.

تاريخ التدقيق الداخلي ومعلومات أساسية عنه:

يمكن لكبار المديرين التنفيذيين فهم التدقيق الداخلي ومجالاته المعرفية الأساسـية على نحو أفضل من خـلال معرفتهم لبعض المعلومات عن المنظمة المهنية للمدققين الداخليين، IIA، ومعاييرها المهنية المنشورة. وقد قامت تلك المنظمة المهنية بتعريف التدقيق الداخلي على النحو التالي:

> "التدقيق الداخلي هو وظيفة تقييم مسـتقلة مصممة داخل المنظمة لفحص وتقييم أنشطتها باعتبارها خدمة للمنظمة."

سـيكون هذا التعريف أكثر وضوحاً عندما نركز على مصطلحاته الأساسـية. حيث يشير التدقيـق إلى مجموعة متنوعة من الأفكار التي يمكن أن يُنظر إليها من زاوية ضيقة للغاية، مثل التحقق من الدقة الحسابية أو الوجود الفعلي للسجلات المحاسبية، أو على نطاق أوسع كالمراجعات والتقييمات التي تتم على العديد من المسـتويات التنظيمية. سـيتم استخدام مصطلح التدقيق طيلة هذا الفصل ليشمل هذه المجموعة المتنوعة من مستويات الخدمة،

التي تمتد من الفحص التفصيلي وحتى الوصول إلى التقييمات العالية المستوى. أما مصطلح الداخلي فيقصد به أن العمل يتم داخل المؤسســة، بواسطة الموظفين العاملين فيها، بعكس المدققين الخارجيين الذين يتم تنفيذ أعمالهم بواســطة محاســبين قانونيين أو أطراف أخرى مــن خارج المؤسســة، كالمنظمات أو الجهــات الرقابية الحكومية، التــي لا تعتبر جزءاً من المؤسسة.

يشــتمل الجزء المتبقي من هذا التعريف الخــاص بالمنظمة المهنية للمدققين الداخليين IIA والخاص بالتدقيق الداخلي على مصطلحات أخرى هامة تنطبق على هذه المهنة وهي:

- مســتقلة: هو المصطلح الذي يشــير إلى أن التدقيق الداخلي خال من أيةِ قيود يمكن أن تحد بشــكل كبير من نطــاق وفاعلية أي عمليــة مراجعة يقوم بها المدقــق الداخلي أو تؤثــر في التقارير التي يتم إعدادها بعد ذلك بشــأن المحصلة النهائيــة الخاصة بالنتائج والاستنتاجات.
- التقييــم: هو مصطلح يؤكد ضرورة إجــراء التقييم الذي يعد بمثابة قوة الدفع للمدققين الداخليين عند قيامهم بوضع استنتاجاتهم.
- مصممة: هو مصطلح يؤكد أن التدقيق الداخلي عبارة عن وظيفة رسمية محددة داخل المؤسسة الحديثة.
- فحص وتقييم: مصطلحان يصفان الأدوار النشــطة التي يقــوم بها المدققون الداخليون، بداية بالاستفسارات الخاصة بـتقصي الحقائق ثم بالتقييمات التحكيمية النزيهة.
- أنشــطتها: هو مصطلح يؤكد النطاق الواسع لولاية أو ســلطة الأعمال الخاصة بالتدقيق الداخلي والذي يسري على جميع أنشطة المؤسسة الحديثة.
- الخدمة: مصطلح يشير إلى أن المساعدة ومد يد العون إلى لجنة التدقيق والإدارة وغيرهم من أعضاء المؤسسة هي الغاية الحقيقية النهائية من جميع أعمال التدقيق الداخلي.
- المنظمــة: مصطلح يؤكد أن النطاق الإجمالي لخدمة التدقيق الداخلي يشــمل المؤسســة بأكملهــا، متضمناً ذلك جميــع الموظفين ومجلــس الإدارة ولجنة التدقيق والمســاهمين وغيرهم من أصحاب المصالح.

كـما يجب الاعتراف أيضاً بأن إدارة التدقيق الداخـلي تعد بمثابة هيئة رقابية تنظيمية داخـل المؤسسـة تعمل من خلال قيـاس وتقييم فاعليـة الضوابط الأخـرى. فالمدققون الداخليـون الذيـن يقومون بأداء أعمالهم بفاعلية وكفـاءة يُصبحون خبراء في عمل أفضل التصاميم والتطبيقات الممكنة لجميع أنواع الضوابط والممارسـات المفضلة. وتتضمن هذه الخـبرة فهم أوجه الترابط بـين الضوابط المختلفة وأفضل تكامـل ممكن فيما بينها داخل النظام الـكلي للرقابة الداخلية. وبذلك تعد الرقابة الداخلية بمثابة الباب الذي من خلاله يأتي المدققون الداخليون لدراسـة وتقييم جميع أنشطة المنظمة وتوفير أقصى قدر ممكن من الخدمات للمؤسسة. لا يمكن التوقع بأن يكون المدققون الداخليون متساوين - بغض النظر عن كثرتهم - في الخبرات الفنية والتشـغيلية الخاصة بالعديد من الأنشطة المختلفة للمؤسسـة. لكن ومع ذلك، يمكن للمدققين الداخليين مساعدة هؤلاء الأفراد المسؤولين في تحقيق نتائج أكثر فاعلية من خلال تقييم الضوابط القائمة وتوفير أسـاس للمسـاعدة على تحسين تلك الضوابط وكذلك الممارسات الخاصة بـحوكمة تقنية المعلومات ذات الصلة.

بعض المعلومات الأساسية عن دور التدقيق الداخلي قد تكون ذات فائدة. فعلى الرغم من الأصول التاريخية القديمة للتدقيق الداخلي، فإنه لم يتم إدراك أو الاعتراف بمدى أهميته مـن قبل العديد من المؤسسـات ومدققيها الخارجيين حتى ثلاثينيـات القرن الماضي. فقد كان السبب الرئيسي للاهتمام بمهنة التدقيق الداخلي والاعتراف به يعود في المقام الأول إلى إنشاء هيئة الأوراق المالية والبورصة الأمريكية (SEC) في عام ١٩٣٤ وتغير أهداف وتقنيات التدقيق الخارجـي في ذلك الوقت. وفي هذا الوقت تماماً، تعرضت الولايات المتحدة وبقية دول العـالم لكسـاد depression اقتصادي كبير بكل المقاييس، والذي كان أكثر شـدة من الركـود recession العالمي الكبير الذي بدأ في عـام ٢٠٠٨. وفي إجراء تشريعي تصحيحي، طالبت هيئة الأوراق المالية والبورصة الأمريكية (SEC) المؤسسات المسجلة بضرورة تقديم بيانات مالية معتمدة من مدققي حسابات مستقلين. كما دفع هذا المطلب أيضاً الشركات إلى القيـام بإنشـاء إدارات التدقيـق الداخلي، ولكـن مع الحفاظ على الهـدف الرئيسي في مسـاعدة مدققيها المسـتقلين. حيث قام المدققون الماليّون الخارجيون وقتها بالتركيز على إبداء آرائهم حول نزاهة القوائم المالية للمؤسسة بدلاً من التركيز على كشف نقاط الضعف الموجـودة في الرقابة الداخلية. وقد حثت قواعـد هيئة الأوراق المالية والبورصة الأمريكية

(SEC) على التدقيق القائم على عينة محدودة من المعاملات، إلى جانب المزيد من الاعتماد على إجراءات الرقابة الداخلية.

وقد كان المدققون الداخليون في ذلك الوقت معنيين في المقام الأول بفحص السجلات المحاسبية والكشف عن الأخطاء والمخالفات المالية. وكانوا في كثير من الأحيان أكثر قليلاً من مساعدين لمدققي الحسابات الخارجيين المستقلين، والمكلفين بتنفيذ التسويات المحاسبية الروتينية أو بمثابة أفراد للدعم المكتبي. وقد استمرت آثار هذا التعريف القديم للتدقيق الداخلي في بعض الأماكن حتى أوائل السبعينيات من القرن الماضي. على سبيل المثال، حتى سبعينيات القرن الماضي كان "المدققون" العاملون في العديد من المنظمات التي تمارس عمليات البيع بالتجزئة هم الأشخاص الذين يقومون بعد النقدية وترصيد آلات تسجيل النقدية (تذكر تلك؟) في نهاية كل يوم عمل.

وعلى الرغم من أنه هناك أصواتاً أخرى تطالب بضرورة عمل شيء لتحسين إمكانيات المدققين الخارجيين والاستفادة منها بشكل أفضل، فإن هناك أموراً قد بدأت بالفعل بعد أن أتم فيكتور ز. برينك Victor Z. Brink أطروحته الجامعية عن التدقيق الداخلي قبل الخروج للخدمة في الحرب العالمية الثانية. وبعد انتهاء الحرب، عاد برينك لتنظيم ورئاسة التدقيق الداخلي لشركة فورد موتور (Ford Motor)، وقد نُشرت أطروحته الجامعية في الطبعة الأولى من الكتاب المرجعي القياسي المتاح الآن عن هذا الموضوع، التدقيق الداخلي الحديث[١] (Modern Internal Auditing).

وقد انطلق معهد المدققين الداخليين (IIA) في الوقت نفسه تقريباً، في عام ١٩٤١، من خلال تأسيس الفرع الأول له في نيويورك، وسرعان ما تبعه إنشاء فرع آخر في شيكاغو. وقد تم تشكيل المنظمة من قبل الأشخاص الذين تم منحهم لقب "مدقق داخلي" من قبل مؤسساتهم، والذين يريدون تبادل الخبرات والمعارف المكتسبة مع الآخرين في هذا المجال المهني الجديد. وبذلك تمت عملية ولادة هذه المهنة وارتفاع مكانتها وأهميتها منذ ذلك الحين.

كانت مهنة التدقيق الداخلي الحديث في أربعينيات القرن الماضي تتطلب مجموعة من المهارات المهنية المختلفة تماماً عما هي عليه اليوم. على سبيل المثال، لم تكن بعض الأجهزة الإلكتروميكانيكية وأنشطة مختبرات الأبحاث ونظم الحاسب الرقمية موجودة في

ذلك الوقت. هذا بالإضافة إلى عدم حاجة المؤسسات في ذلك الوقت إلى مبرمجي الحاسب الآلي حتى بدأت تصبح بعض آلات الجدولة البدائية مفيدة في حفظ السـجلات وغيرها من المهام الحسـابية والمحاسبية. وبالمثل، كانت مؤسسات الاتصالات الهاتفية بدائية جداً، فقد كان يقوم مشغلو لوحة التوزيع (المقسم) بتحويل جميع المكالمات الواردة إلى عدد محدود مـن الهواتف المكتبية. أما اليوم، فلدينا بالطبع موارد لتقنية المعلومات ترتبط جميعها من خلال الشـبكة الإلكترونية الضخمة للإنترنت المكونة من الاتصالات السـلكية واللاسلكية في كل أنحاء العالم. وقد أدى التعقيد المتزايد للأعمال وغيرها في المؤسسات الحديثة إلى الحاجة إلى مدققين داخليين ليصبحوا متخصصين أكثر من أي وقت مضى في مختلف ضوابط الأعمال.

لقـد لعب هؤلاء المدققـون الداخليون الأوائل في كثير من الأحيان دوراً محدوداً جداً في المؤسسـات التابعين لها، في ظل مسـؤولياتهم المحدودة نسبياً من مجموع الطيف الإداري. فالمدقـق الداخـلي الأول كان يُنظر إليه غالباً على أنه مراجع للسـجلات المالية وأنه ضابط شرطـة أكثر من كونه زميلاً في العمل. في بعض المؤسسـات، كان لـدى المدققين الداخليين مسـؤوليات كبيرة في تسـوية الشـيكات الملغاة للمرتبات مع البيانات المصرفية أو مراجعة الحسابات الموجودة في المستندات النظامية للأعمال.

ومع مرور الوقت، ازداد حجم وشدة تعقيد العمليات التشغيلية في العديد من مؤسسات الأعمال، الأمر الذي استحدث مشاكل إدارية وضغوطاً جديدة على الإدارة العليا. وقد كانت ردة الفعل الطبيعية لذلك، هو إدراك العديد من كبار المديرين أن هناك احتمالات لتحسين الاسـتفادة من المدققين الداخليين. كان هناك بالفعل أفراد تم تعيينهم في وظيفة التدقيق الداخلي للمؤسسـة، ويبدو أنه كان هناك سـبب وجيه للحصول على قيمة أكبر من هؤلاء الأفراد مع زيادة طفيفة نسبياً في التكلفة.

وفي الوقت نفسه، أدرك المدققون الداخليون هذه الفرص، وقاموا باستحداث العديد من أنواع الخدمات الجديدة. وبذلك أخذ المدققون الداخليون على عاتقهم تدريجياً مسؤوليات أكبر وأكثر تركيزاً على الإدارة في أعمالهم. ولأن التدقيق الداخلي كان في البداية موجهاً نحو المحاسـبة إلى حد كبير، فقد كان الشعور بهذا الاتجاه التصاعدي بداية في مجالات المحاسبة والرقابة المالية. فبدلاً من مجرد التبليغ عن المخالفات المحاسـبية ذات الصلة - مثل بعض

الوثائــق التي تخلو من توقيع المشرف - بدأ المدققون الداخليون بالاستفســار عن عمليات الرقابة الشــاملة التي هم بصدد مراجعتها. ومن ثم، بدأ عمل تقييم التدقيق الداخلي يمتد ليشمل العديد من المجالات غير المالية في المؤسسة.

وقد تســببت قواعد ومبادرات الأعمال الجديدة في الولايات المتحدة، مثل إطار الرقابة الداخليــة (COSO)، الذي تم الحديث عنه في الفصل الرابع من هذا الكتاب، أو متطلبات قانون ســاربينز أوكســلي (SOx)، الموضحة في الفصــل الثاني من هذا الكتــاب، في الزيادة المســتمرة للحاجة إلى خدمات المدققين الداخليين. وبالإضافة إلى ذلك، فإن بعض المؤثرات البيئية الحديثة قد أوجدت احتياجات جديدة في مجالات مثل الحماية من المخاطر الصناعية وتقديم الدعم لبرامج مراقبة الجودة ومســتويات مختلفة لمسؤوليات العمل، متضمناً ذلك المعايير الأخلاقية. هذه الحاجة إلى المعايير الأخلاقية تشمل معايير أعلى لحوكمة الشركات، وزيادة مشــاركة مجالــس الإدارة، ولجان التدقيق التابعة لها، ودوراً أكثر نشــاطاً لأصحاب المصالح، وقدراً أكبر من الاستقلالية للمحاسب القانوني الخارجي.

أما اليوم، فقد توســعت أنشــطة التدقيق الداخلي لتصل إلى جميع المجالات التشغيلية للمؤسســة وقــد حجزت لهــا مكاناً يحظــى بالتقدير والاحــترام على أنه جــزء من أعمال ومجهــودات الإدارة العليا. إن المدقق الداخلي اليوم يخدم وبشــكل رســمي وفعال لجنة التدقيق التابعــة لمجلس الإدارة، وإن مدير التدقيق الداخلي (CAE) اليوم لديه مســتوى مبــاشر وفعال للتواصل مع تلك اللجنة نفســها الخاصة بالتدقيــق، وإن هذا الوضع العام يعكــس تقدماً كبيراً في نطــاق تغطية التدقيق الداخلي ومســتوى الخدمة لجميع مجالات المؤسسة. إن مهنة التدقيق الداخلي نفسها، من خلال تنميتها الذاتية وتطبيقها كما ينبغي، أســهمت في تحقيق هذا التقدم، وتمهيد الطريق لاستمرار الاتجاه التصاعدي لها. فهي الآن تعد مكوناً هاماً من مكونات العمليات الفعالة لحوكمة تقنية المعلومات.

التدقيق الداخلي ومدقق تقنية المعلومات:

لقــد تحدثنا عن تطــور كل من مهنة التدقيق الداخلي ومعهــد المدققين الداخليين IIA كذلــك، وهو المنظمة المهنية العالمية للتدقيــق الداخلي. وعلى الرغم من أنه يجب على أي منظمــة مهنية أن تقوم بتقييم أو تقدير احتياجــات أعضائها في ضوء الظروف المتغيرة، فإن

مـــن الممكن أن تكـــون هذه التغيرات في بعـــض الأحيان بطيئة بعض الـــشيء. أصابت تلك التغيرات معهد المدققين الداخليين (IIA) في غضون فترة النمو الهائل في نظم وعمليات تقنية المعلومات، والذي ربما يكون قد بدأ في أوائل السبعينيات من القرن الماضي. قد أدرك في ذلك الوقت عدد كبير ومتزايد من المدققين الداخليين أن تلك النظم والعمليات الجديدة الخاصة بتقنية المعلومات قد قدمت مجموعة واســعة من القضايا الجديدة للرقابة الداخلية، إلا أن المنظمة المهنية للتدقيق الداخلي التابعين لها لم تقدم الإرشادات أو الدعم الفني الكافي.

تم تشـــكيل المنظمة المهنية الجديدة، التي ســـميت بعد ذلك بجمعيـــة مدققي معالجة البيانات الإلكترونيـــة EDP Auditors Association، لدعم هؤلاء العاملين الجدد بالتدقيق الداخـــلي. ويرمـــز الاختصـــار EDP إلى معالجة البيانـــات الإلكترونيـــة (Electronic Data Processing)، وهـــو أحد المصطلحـــات القديمة لنظم وعمليات تقنيـــة المعلومات. ويُعْرَف هؤلاء المهنيون اليوم بأنهم مدققو تقنية المعلومات كما يطلق على المنظمة المهنية الرئيســـية التابعـــين لها الآن اســـم جمعية ضبط وتدقيق نظـــم المعلومـــات (Information Systems Audit and Control Association)، وهـــي منظمـــةٌ مهنيةٌ هامـــة في مجال حوكمة تقنية المعلومـــات وقد تقدم ذكرها للمرة الأولى في الفصل الخامس من هذا الكتاب. يكون مدققو تقنيـــة المعلومات غالبـــاً متخصصين في الإدارات التقليدية للتدقيـــق الداخلي، ولكن يرتبطون كثيراً بشركات المحاســـبة القانونية الرئيســـية أو العمل كذلك بصفة مستشـــارين خصوصيين. ولهم دور هام جداً في وضع ومتابعة العمليات الفعالة لحوكمة تقنية المعلومات في المؤسسة.

يتعين على كبار مديري الأعمال فهم أدوار ومســـؤوليات المدققين الداخليين فيما يخص حوكمـــة تقنية المعلومات في مؤسســـاتهم، مع إيلاء المزيد من الاهتـــمام بأخصائيي تدقيق تقنية المعلومـــات التابعين لها. فبالإضافة إلى الدور الذي يلعبه التدقيق الداخلي في تقديم التقارير إلى لجنة التدقيق التابعة لمجلس الإدارة، له دور ووظيفة خاصة جداً في المؤسســـة. فهو بشـــكل عام يعمل بصفته نوعاً من أنواع الوظائف التعاونية، فهو يقوم بوضع الجدول الزمني والأنشـــطة الخاصة به غير أنه يدعم الإدارة العليا من خلال المراجعات والأنشـــطة والتقييمات. وســـتتحدث الأقسام التالية عن بعض المسؤوليات الهامة للتدقيق الداخلي في حوكمة تقنية المعلومات المؤسسية.

أنشطة التدقيق الداخلي ومسئولياته المرتبطة بحوكمة تقنية المعلومات:

"كن حذراً، فالمدققون قادمون!" لقد شاع استخدام هذا النوع من التحذيرات في الماضي القريب عندما كانت إدارة التدقيق الداخلي تُخْطِر مدير المؤسسة بأنهم قاموا بإعداد جدول زمني لمراجعة أحد التطبيقات أو العمليات الخاصة بتقنية المعلومات بشكل عام أو بعض المجالات الأخرى ذات الاهتمام. وقد كانت ردة الفعل الطبيعية وقتها لصاحب عمليات تقنية المعلومات هي أن يقول بأن عمليات التدقيق المخطط لها قد تمت جدولتها في "الوقت غير المناسب" وذلك للعديد من الأسباب. ومع ذلك، كان موعد التدقيق الداخلي المخطط له قد تم تحديده قريباً، وأن التدقيق الداخلي سيقوم بإجراء المراجعات الخاصة بهم، وسيتم إعداد تقارير عن النتائج، وسيكون المدير وقتها هو المسؤول عن الرد على جميع الملاحظات الخاصة بالتدقيق وتنفيذ الإجراءات التصحيحية الموصى بها.

إن كبار المديرين بحاجة إلى فهم وإدراك مجمل عملية التدقيق الداخلي والكيفية التي يتم من خلالها جدولة وتنفيذ عمليات التدقيق الداخلي ومن ثم القيام بإعداد التقارير الخاصة بها. وبالرغم من احتمالية وجود العديد من الاختلافات، اعتماداً على حجم ودرجة تعقيد المنظمة وأهداف عملية التدقيق، فإن العملية النموذجية للتدقيق الداخلي تحتاج إلى جدولة عملية المراجعة والقيام بتقييم المخاطر وتنفيذ إجراءات التدقيق الضرورية، ومن ثم إعداد تقارير عن نتائج التدقيق وإرسالها إلى إدارة ولجنة التدقيق. لسنا هنا بصدد وصف الكيفية التي يتم من خلالها تنفيذ عمليات التدقيق الداخلي، ولكننا نهدف بشكل عام إلى تحقيق فهم لهذه العملية. ومع ذلك فالنقطة الأساسية هنا هي أن الأشخاص الذين يقومون بتنفيذ عمليات التدقيق الداخلي لا ينبغي أن يتصرفوا بصفة استشاريين داخليين. وكما وضحنا في وصفنا المختصر للمعايير المهنية للتدقيق الداخلي في القسم التالي، فإنه يتعين على المديرين التنفيذيين الذين لم يشاركوا بشكل مباشر في عملية التدقيق الداخلي أن يدركوا أن الدور الرئيسي للتدقيق الداخلي هو فحص ومراجعة واختبار الضوابط الداخلية والعمليات المرتبطة بها. أما إذا تصرفت وحدة التدقيق الداخلي كما لو كانت هيئة استشارية داخلية، وجب أن يتم اتخاذ ترتيبات منفصلة، وفي مثل هذه الحالة يتعين على جميع الأطراف أن تدرك أن الأنشطة الاستشارية الداخلية منفصلة ومختلفة عن أنشطة التدقيق الداخلي.

عملية التدقيق الداخلي: التخطيط لعمليات التدقيق الداخلي ومنح الترخيص الخاص بها:

إن إدارة التدقيق الداخلي في المؤسسة النموذجية ليست إدارة منفصلة، مثل إدارة المشتريات أو حساب المقبوضات أو الإدارة الهندسية، وإنما إدارة التدقيق الداخلي وكذلك رئيس التدقيق الداخلي - يسمى عادة مدير التدقيق الداخلي (CAE) - هو من يقوم بإعداد التقارير وإرسالها مباشرة إلى لجنة التدقيق التابعة لمجلس الإدارة. وقد تم فرض هذا المطلب في الولايات المتحدة، من قبل هيئة الأوراق المالية والبورصة الأمريكية (SEC). وعلى الرغم من أنه قد يكون لعملية التدقيق الداخلي علاقة اسمية بعملية إعداد التقارير وإرسالها إلى المدير المالي (CFO) أو بعض الوظائف الإدارية الأخرى، فإنه يجب أن يكون للتدقيق الداخلي علاقة مستقلة مع لجنة التدقيق.

ويتم التكليف للقيام بأنشطة التدقيق الداخلي من خلال وثيقة رسمية تعرف بميثاق التدقيق الداخلي، والتي تتم الموافقة عليها من قبل لجنة التدقيق، ويُمنح فريق التدقيق الداخلي السلطة الكاملة لإجراء مراجعات مستقلة وفحص للمواد. فمن منظور حوكمة تقنية المعلومات، على سبيل المثال، فإن وثيقة الميثاق تُعْطِي فريق التدقيق الداخلي السلطة للدخول على العمليات التشغيلية لمركز البيانات ومراجعة التقارير والمواد السرية الأخرى التي تعد جزءاً من عمليات التدقيق المخطط لها.

الشكل التوضيحي (١٩-١) يُعد مثالاً لميثاق التدقيق الداخلي لإحدى الشركات، وهي الشركة العالمية لمنتجات الحاسب (Global Computer Products)، وهو نموذج الشركة الذي تم استخدامه سابقاً. إذ يبين هذا الميثاق بوضوح "تعليمات التقدم marching orders" الخاصة بإحدى إدارات التدقيق الداخلي. وعندما يكون لدى المسؤول التنفيذي للشركة أي شكوك تتعلق بأنشطة وسلطة المدققين الداخليين، ينبغي عليه أن يطلب الاطلاع على نسخة من ميثاق التدقيق الداخلي الخاص بهم. فإذا تبين أن هذا الميثاق قد أهمل بعض المجالات كالقضايا المتعلقة بحوكمة تقنية المعلومات أو أنه منتهي الصلاحية، فإنه يتعين على المسئول التنفيذي أن يطلب من رئيس لجنة التدقيق CAE الشروع في إجراءات تحديث الميثاق.

شكل توضيحي (١٩-١)

عينة لميثاق التدقيق الداخلي

إدارة التدقيق الداخلي
ميثاق تصريح
مهمة التدقيق الداخلي: إن مهمة التدقيق الداخلي للشركة العالمية لمنتجات الحاسب (Global Computer Products)هو التأكد من أن عمليات الشركة تتبع معايير عالية، وذلك من خلال توفير إدارة ضمان مستقلة وموضوعية وتقديم المشورة بشأن أفضل الممارسات. فباستخدام نهج منظم ومنضبط، يساعد التدقيق الداخلي الشركة العالمية لمنتجات الحاسب على تحقيق أهدافها من خلال تقييم وتحسين فاعلية إدارة المخاطر والرقابة الداخلية وعمليات الحوكمة.
الاستقلالية والموضوعية: لضمان الاستقلالية فإن تقارير التدقيق الداخلي تُقدَّم مباشرة إلى لجنة التدقيق التابعة لمجلس الإدارة، وللحفاظ على الموضوعية، فإن التدقيق الداخلي لا يشارك في عمليات التشغيل اليومية للشركة أو إجراءات الرقابة الداخلية.
النطاق والمسؤوليات: يشمل نطاق عمل التدقيق الداخلي مراجعة إجراءات إدارة المخاطر والرقابة الداخلية ونظم تقنية المعلومات وعمليات الحوكمة. ويشمل هذا العمل أيضاً الاختبار الدوري للمعاملات ومراجعة أفضل الممارسات والتحقيقات الخاصة وتقييم المتطلبات القانونية والتنظيمية والقياسات للمساعدة في منع واكتشاف الاحتيال. **للوفاء بمسؤولياتها، يتعين على التدقيق الداخلي:** - تحديد وتقييم المخاطر المحتملة لعمليات تشغيل المؤسسة. - مراجعة مدى كفاية الضوابط الموضوعة لضمان الامتثال للسياسات والخطط والإجراءات وأهداف العمل. - تقييم موثوقية وأمن المعلومات المالية والإدارية والنظم الداعمة وعمليات التشغيل التي تُنْتِج هذه المعلومات. - تقييم وسائل حماية الأصول. - مراجعة العمليات القائمة واقتراح تحسينات لها. - تقييم استخدام الموارد فيما يتعلق بالاقتصاد والكفاءة والفاعلية. - متابعة التوصيات للتأكد من أن الإجراءات التصحيحية الفعالة يتم اتخاذها وتطبيقها فعلاً. - تنفيذ التقييمات أو التحقيقات أو المراجعات المتعلقة بموضوع ما والمطلوبة من قبل لجنة التدقيق والإدارة.

سلطة التدقيق الداخلي: مـــن أجل تعزيز ضوابط فعالة بتكلفـــة معقولة، يُصَرَّح للتدقيق الداخلي، في حدود نطاق أنشـــطته، بأن يقوم بـ: - دخـــول جميع مناطق عمليات التشـــغيل للشركـــة العالمية لمنتجات الحاســـب والحصول على أي وثائق وسجلات تعتبر ضرورية لإتمام المهام المكلفة بها. - مطالبـــة جميع أعضاء طاقم العمـــل والإدارة بتزويدهم بالمعلومات والإيضاحـــات المطلوبة خلال فترة زمنية معقولة.
المساءلة: يتعين على التدقيق الداخلي أن يقوم، بالتنسيق مع إدارة ولجنة التدقيق، بإعداد الخطة السنوية للتدقيق التي تعتمد على مخاطر العمل ونتائج التدقيقات الداخلية الأخرى، ومدخلات الإدارة. ويجب أن تُقدَّم الخطة للإدارة العليا، متضمناً ذلك المستشار العام، للموافقة عليها من قِبل لجنة التدقيق. وإن كان هناك أي تعديلات ضرورية على الخطة ينبغي إرسالها والموافقة عليها من قِبل لجنة التدقيق. إن التدقيق الداخلي هو المســـؤول عن التخطيط والتوجية وإعداد وتقديم التقارير ومتابعة مشـــاريع التدقيق المدرجة في خطة التدقيق واتخاذ قرار بشـــأن نطاق وتوقيت هذه التدقيقات. وســـيتم الإبلاغ عن نتائـــج كل عملية من عمليات التدقيـــق الداخلي من خلال تقرير التدقيـــق التفصيلي الذي يلخص أهداف ونطـــاق التدقيـــق وكذلك الملاحظـــات والتوصيات. وفي جميع الحالات، ســـيضطلع عمـــل المتابعة بضمان الاستجابة الكافية لتوصيات التدقيق الداخلي. وسوف يُقدِّم التدقيق الداخلي أيضاً تقريراً سنوياً إلى الإدارة العليا وإلى لجنة التدقيق حول نتائج أعمال التدقيق، متضمناً ذلك التعرض للمخاطر المؤثرة وقضايا الرقابة.
المعايير: يلتزم التدقيق الداخلي للشركة العالمية لمنتجات الحاســـب بالمعايير والممارسات المهنية الصادرة عن معهد المدققين الداخليين ومعهد حوكمة تقنية المعلومات كذلك.

بينـــما قد تُلْـــزِم أو تطلب لجنة التدقيق من الرئيس التنفيـــذي للتدقيق الداخلي CAE وإدارة التدقيـــق الداخلي التابعين لهـــا، القيام بإجراء إحدى المراجعـــات المحددة للتدقيق الداخـــلي؛ يقوم التدقيق الداخلي عادة من خلال التقييمات المســـتمرة للمخاطر أو طلبات الأعضاء الآخرين في الإدارة أو من خلال خبراتها المكتسبة من عمليات أخرى كانت قد أجرتها للتدقيـــق الداخلي - بتطويـــر خطط قصيرة الأجل وأخرى طويلة الأجـــل لعمليات التدقيق الداخـــلي التي تُخطط لتنفيذها خلال الفـــترة القادمة. فبالاعتماد على هذه الخطة وكذلك عـــلى عمليات التدقيـــق المكتملة في الماضي القريب، يتعين عـــلى الرئيس التنفيذي للتدقيق

CAE اتخــاذ جميع التدابير والترتيبات الضرورية الخاصة بموظفي التدقيق الداخلي وغيرها من الموارد لتنفيذ هذا البرنامج الخاص بعمليات التدقيق الداخلي المخطط لها للمؤسسة.

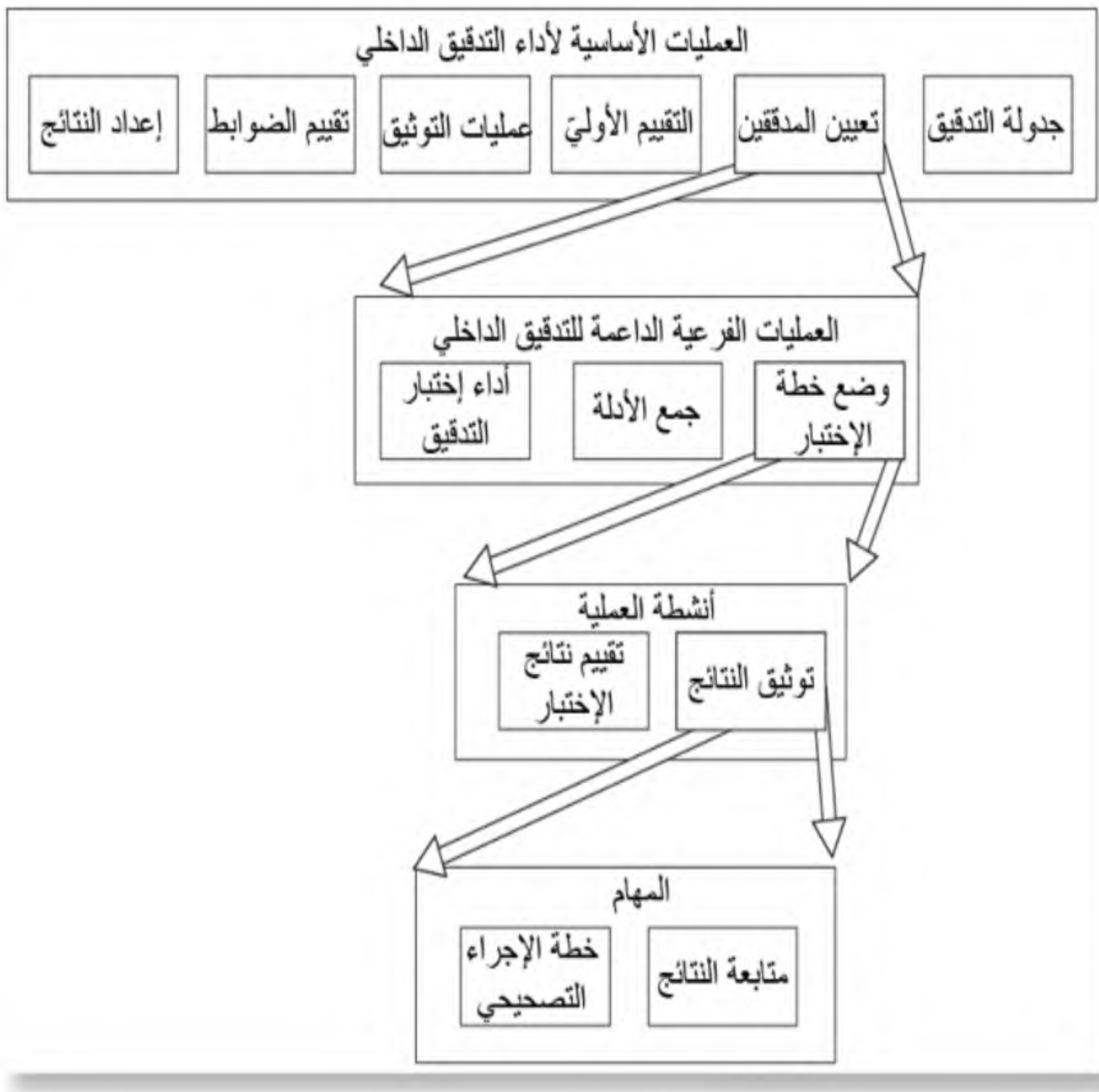
عملية التدقيق الداخلي: تدشين عملية التدقيق الداخلي:

يوضح الشــكل التوضيحي (١٩-٢) العمليات اللازمة لإجراء عملية التدقيق الداخلي المكونــة من أربعة مراحل أو خطوات مختصرة. ومع أن الخطة الســنوية تســتلزم أن يتــم إجــراء التدقيق الداخــلي في أحد المناطــق ، فإنه من باب المجاملة، وبشــكل عام تقتــضي أن يقوم التدقيق الداخلي بالعمل مــع المنطقة التي يتم مراجعتها لجمع بعض التفاصيــل الأولية حول المنطقة محل المراجعــة وجدولة عملية التدقيق. هناك العديد من النشــاطات لــكل مرحلة من المراحل الموضحة بالشــكل. على ســبيل المثال، تدعو المرحلة ذات المستوى الأعلى إلى:

- **جدولة التدقيق:** بعد أن تم وضع الخطة الســنوية الشاملة للتدقيق والمعتمدة من قِبل لجنة التدقيق، يجب أن يتم وضع جدول زمني لعملية التدقيق المحددة، مع الأخذ بعين الاعتبار الاحتياجات الخاصة بمــوارد التدقيق واعتبارات الوقت الخاصة بالجهة الخاضعة للتدقيق، وغيرها من العوامل.
- **تعيــين المدققــين:** يكون هنــاك غالباً ندرة في المــوارد البشرية العاملــة في تدقيق تقنية المعلومات. لذا يجب إيــلاء المزيد من الحرص والاهتمام لعملية تعيين أخصائيي تدقيق تقنية المعلومات للمهام المناســبة، في حين أن المدققــين الداخليين ذوي المهارات الأخرى ينبغي أن يتم تعيينهم في الأماكن الأنسب لهم.
- **إجــراء التقييمات الأوليــة للتدقيق:** قد يقوم التدقيق الداخــلي بجدولة عمليات المراجعة الخاصة بتقييم الضوابط الداخلية لإحدى النظم أو العمليات، ولكن قبل البدء في العمليات الفعليــة للتدقيق، يكون من الضروري القيام بجمع المزيد من المعلومات المتعلقة بالمنطقة المراد مراجعة عملياتها وإجراء بعض التقديرات الأولية حول مداها وعمقها وجميع الضوابط الداخلية والمخاطر المرتبطة بها، وبالأساليب المستخدمة لتقييم المنطقة المراد مراجعتها.

شكل توضيحي (١٩-٢)

عملية أداء التدقيق الداخلي



• **توثيق العمليات الخاصة بالمنطقة التي يتم تدقيقها:** يعد التوثيق المناسب مطلباً رئيسياً لجميع أعمال التدقيق الداخلي. ولا يكفي القول بأن لدى إحدى العمليات ضوابط داخلية كافية. فالمدقق الداخلي يجب عليه أن يقوم بجمع الأدلة الوثائقية لإثبات أن هذه الضوابط كافية في الوقت الذي يقوم فيه المدقق بالمراجعة.

- **تقييــم الضوابط الداخليــة:** إن تقييم الضوابط الداخليــة في الحقيقة هو جوهر عملية التدقيق الداخلي. فالمدقق الداخلي يأخذ الضابط الداخلي الذي هو بصدد تقييمه ويقوم بوضع خطة اختبار لتقييم هذا الضابط. وقد يحتاج ذلك إلى جمع أدلة التدقيق وإجراء اختبارات التدقيق، كما هو مبين في المستوى التالي للعمليات الموضحة بالشكل.
- **تحضير وإعداد النتائج:** يقوم المدقق الداخلي باختبار وتقييم الضوابط الداخلية من خلال استخدام مجموعة متنوعة من الأساليب، والتي تبدأ من الاختبار الرسمي للمعاملات إلى الحصــول على الانطباعات من خــلال المقابلات أو الملاحظات، وهي تســمى غالباً نتائج التدقيــق الداخــلي. وقد تجد نتائــج وملاحظات الاختبار هذه طريقهــا أخيراً إلى تقرير رسمي للتدقيق الداخلي يلخص تلك النتائج والتوصيات الخاصة بالتدقيق.

لقد قمنا للتو بوصف الخطوات الرئيســية في عمليــة التدقيق الداخلي، فالمدقق الداخلي ســوف يمر بالنمط نفســه من الخطوات في كل منطقة من المناطق التي يقوم بمراجعتها. لا يهدف هذا الفصل إلى تقديم وصف شامل للكيفية التي يتم من خلالها إجراء عملية التدقيق الداخــلي لكبار المســؤولين التنفيذيين، ولكن يهدف إلى إعطاء فهــم للعمليات اللازمة لإجراء التدقيق الداخلي المناسب. ستبقى هذه الخطوات الأساسية هي نفسها سواء أكانت لمراجعة الضوابط المالية لإحدى العمليات أم لمراجعة أحد تطبيقات النظم الخاصة بتقنية المعلومات.

عملية التدقيق الداخلي: مراجعة أدلة التدقيق واختبارها:

يحتــاج الجــزء الأكبر من عملية التدقيق الداخلي إلى جمــع ومراجعة واختبار ما يُطلِق عليه المدققون الداخليون اسم أدلة التدقيق Audit evidence. فقد يسأل المدقق الداخلي عن حالة التوثيــق الخاصة بأحد التطبيقات الجديدة لتقنيــة المعلومات، ويتم إخباره بأن التوثيــق "حديث". فإذا كان النظام أو التطبيــق ثانوياً، فقد يقوم المدقق باعتماد وتدوين تلــك الإجابة والمضي قدماً. في جميــع الأحوال فلكي يكون لدينا أدلة قوية على حداثة ذلك التوثيــق، فقد يقــوم المدقق الداخلي بطلب مراجعة التوثيق الفعــلي للتأكد من وجودها. ولمزيــد من التفاصيل، قد يقوم المدقق الداخلي بالتعمق أكثر في التوثيق وفحص أمور منها على ســبيل المثال مــدى ملاءمة التنقيحات التي تمت عليهــا، أو أن يقوم بإجراء المزيد من الفحوصات المختلفة ليرى ما إذا كانت هذه الوثيقة كافية وداعمة لضوابط النظام.

تتطلب هذه العملية برمتها أن يقوم المدقق الداخلي بتقييم مدى كفاية أدلة التدقيق الموجودة وإجراء بعض التقييمات بناء على عمل التدقيق الداخلي. الشكل التوضيحي (١٩-٣) يبين أنواعاً مختلفة من أدلة التدقيق من الأقوى إلى الأضعف. ويبين العمود الأول أنواع أدلة التدقيق، فتقنية التدقيق الخاصة بمشاهدة ممارسة ما على أرض الواقع تعد أقوى بكثير من مجرد الإخبار عن تلك الممارسة. لا توجد أي مطالبة تتعلق بوجوب دعم كل أعمال التدقيق الداخلي من قِبل أقوى مستويات الأدلة. حيث إن طبيعة التدقيق الداخلي والمخاطر المرتبطة بها تعد من العوامل المُحَدِدَة للمستوى المطلوب لأدلة التدقيق، فإنه يجب دائماً على المدير الأول الذي يعمل مع المدققين الداخليين ويقوم بمعالجة التوصيات الناتجة عنهم أن يأخذ في الحسبان الطريقة التي يستخدمها هؤلاء المدققون في جمع أدلة التدقيقات الداعمة لنتائجهم واستنتاجاتهم الموثقة.

عملية التدقيق الداخلي: تقديم التقارير الخاصة بنتائج التدقيق الداخلي:

يجب أن تُخْتَتَم الأعمال الخاصة بعملية التدقيق الداخلي بتقرير رسمي يصف الأهداف التي من أجلها تمت هذه المراجعة في منطقة ما، وما الإجراءات المتبعة لتقييم الضوابط الداخلية الخاصة بهذه الأهداف التدقيقية، وما الذي تم اكتشافه، وما إذا كانت الضوابط الداخلية الموجودة قد قُيِّمَت بشكل كافٍ أم لا. في معظم الحالات، نجد أن هذه التقارير الخاصة بعملية التدقيق سوف تؤدي إلى توصيات رسمية تتعلق بإجراء تحسينات على الرقابة الداخلية بناء على نتائج التدقيق في المجال الذي تمت مراجعته. وعلى الرغم من أن الممارسات قد تختلف باختلاف المؤسسات، فإن تقارير التدقيق الداخلي عموماً ستحتاج إلى استجابة إدارية رسمية تُقر بنتائج التدقيق الداخلي وتوضح الكيفية التي سيستخدمونها لتصحيح أوجه القصور في الرقابة المبلغ عنها بالتقرير.

شكل توضيحي (١٩-٣)

تصنيفات جوانب قوة التدقيق الداخلي الخاصة بأدلة التدقيق

تصنيفات أدلة التدقيق الداخلي التي تم جمعها	الأدلة الداعمة القوية لاستنتاجات التدقيق	أضعف المستويات لأدلة التدقيق الداخلي
أسلوب التدقيق	الملاحظات / التأكيدات	استفسار
أصل الأدلة	مدعوم	إحصائيات أساسية
العلاقة مع الجهة الخاضعة للتدقيق	إدارة خارجية	مجموعة داخلية
شكل الأدلة	مكتوب / نظام مؤمن	شفهي
تطور الأدلة	رسمي / موثق	غير رسمي
موقع الأدلة	تم إنشاؤه في نظام فعلي	مستمدة من نظام الدعم
مصدر أدلة التدقيق	عمل تدقيق شخصي	مُوَرَّد "مستعمل"

لا يتم تعميم التقارير الخاصة بعملية التدقيق على المؤسسة. فهي تكون عادة موجهة فقــط إلى منطقة محددة من مناطق المؤسســة التي تمت مراجعــة عملياتها وإلى مديريها المباشرين وإلى الإدارة العليا في المؤسسة كذلك، مثل الرئيس التنفيذي والمدير المالي وشريك التدقيق الخارجي ولجنة التدقيق. إن نتائج التدقيق الســيئة لعمليات التشــغيل في إحدى الوحــدات التي تمت مراجعتها ســوف تــؤدي إلى جعل التركيز بالفعــل ينصب على الإدارة للقيام بتصحيح أو إصلاح أوجه القصور في الرقابة الداخلية في تلك الوحدة. وقد يكون ذلك أحد العناصر الهامة في حوكمة تقنية المعلومات.

يُوَاجِــه المدققــون الداخليون غالباً في العديد من المناطق التــي يقومون فيها بمراجعة عملياتها مشــاكل تتعلق بضيق الوقت وقلة الموارد اللازمة لمراجعة وتدقيق جميع المناطق ذات المخاطر العالية في المؤسســات الكبيرة بصورة كافية. فعلى ســبيل المثال، كان مؤلف هــذا الكتاب في فترة من الفــترات يعمل مديراً لإحدى عمليــات التدقيق الداخلي الخاصة بإحدى الشركات الأمريكية الكبرى التي تحتوي على العديد من الوحدات التشــغيلية، وكان لكل وحدة تشــغيلية ثلاثة من مديري التدقيق الداخــلي وما يقارب ثمانين موظفاً يعملون في مجــال التدقيق الداخلي. فعلى الرغم من التحليل المكثف للمخاطر والخطط الســنوية

المنظمــة جيداً لعمليات التدقيق الداخلي، فإنه كان من الصعب اســتكمال جميع عمليات التدقيق المخطط لها وتغطية جميع المخاطر. لذا تم تعديل الخطط وإعادة ملاءمتها بصورة منتظمة بســبب الأزمات الجديــدة للأعمال التي تتطلب المزيد من أنشــطة التدقيق. إن الأنشــطة الاحتيالية المكتشفة حديثاً، على سبيل المثال، من شأنها أن تحول أنشطة التدقيق الداخلي الأخرى للمساعدة في التحقيق في مزاعم الاحتيال على نحو أفضل.

وينبغي على القارئ الذي يريد الحصول على مزيد من المعلومات حول التدقيق الداخلي ودوره في حوكمــة تقنيــة المعلومات أن يعــود إلى كتاب المؤلف الســالف الذكر، التدقيق الداخــلي الحديث لبرينــك (Brink's Modern Internal Auditing). فهذا الكتاب يضع تعريفاً لهيكل المعرفة الشائع للتدقيق الداخلي ، والمجالات الواسعة التي يجب على المدقق الداخلي أن يعرفها ويفهمها.

معايير التدقيق الداخلي الخاصة بحوكمة تقنية المعلومات:

إن المنظمة المهنية للمدققين الداخليين، معهد المدققين الداخليين (IIA)، هي المسؤولة عن إصدار معايير الممارســة والســلوك لجميع المدققين الداخليين، وذلك على أساس عالمي. هذه الإرشــادات الرسمية عبارة عن مزيج من بيانات المعايير الإلزامية المطلوبة والضرورية لممارســة مهنية مستمرة لعملية التدقيق، بالإضافة إلى سلسلة من ممارسات المعايير الموصى بهــا بقوة. إن هذه المعايير الخاصة بمعهد المدققــين الداخليين تذهب إلى ما هو أبعد من أن تكــون مجرد معايير لحوكمة تقنية المعلومات، فهي تغطي نشــاطات التدقيق الداخلي للحوكمة على أســاس واســع. فعلى ســبيل المثال، ينص المعيار 2110. A2 لمعهد المدققين الداخليين IIA والخاص بالأداء على أن:

> "نشاط التدقيق الداخلي يجب أن يُقيّم ويحدد ما إذا كانت حوكمة تقنية المعلومات التابعة للمنظمة تحافظ على إستراتيجيات وأهداف المنظمة وتدعمها."

وعلى الرغم من الأســلوب العام المستخدم في صياغة المعيار، فإنه يطلب في الأساس من المدقق الداخلي أن يقوم بتقييم ما إذا كانت البنية التحتية لتقنية المعلومات في المؤسســة ملائمــة وكافيــة للعمليات التشــغيلية للأعمال والمحافظــة عليها بحيث يتــم إدارة جميع الأهداف الطويلة الأجل للمؤسسة بأكملها بشكل صحيح.

إجراءات التدقيق الداخلي الخاصة بحوكمة تقنية المعلومات:

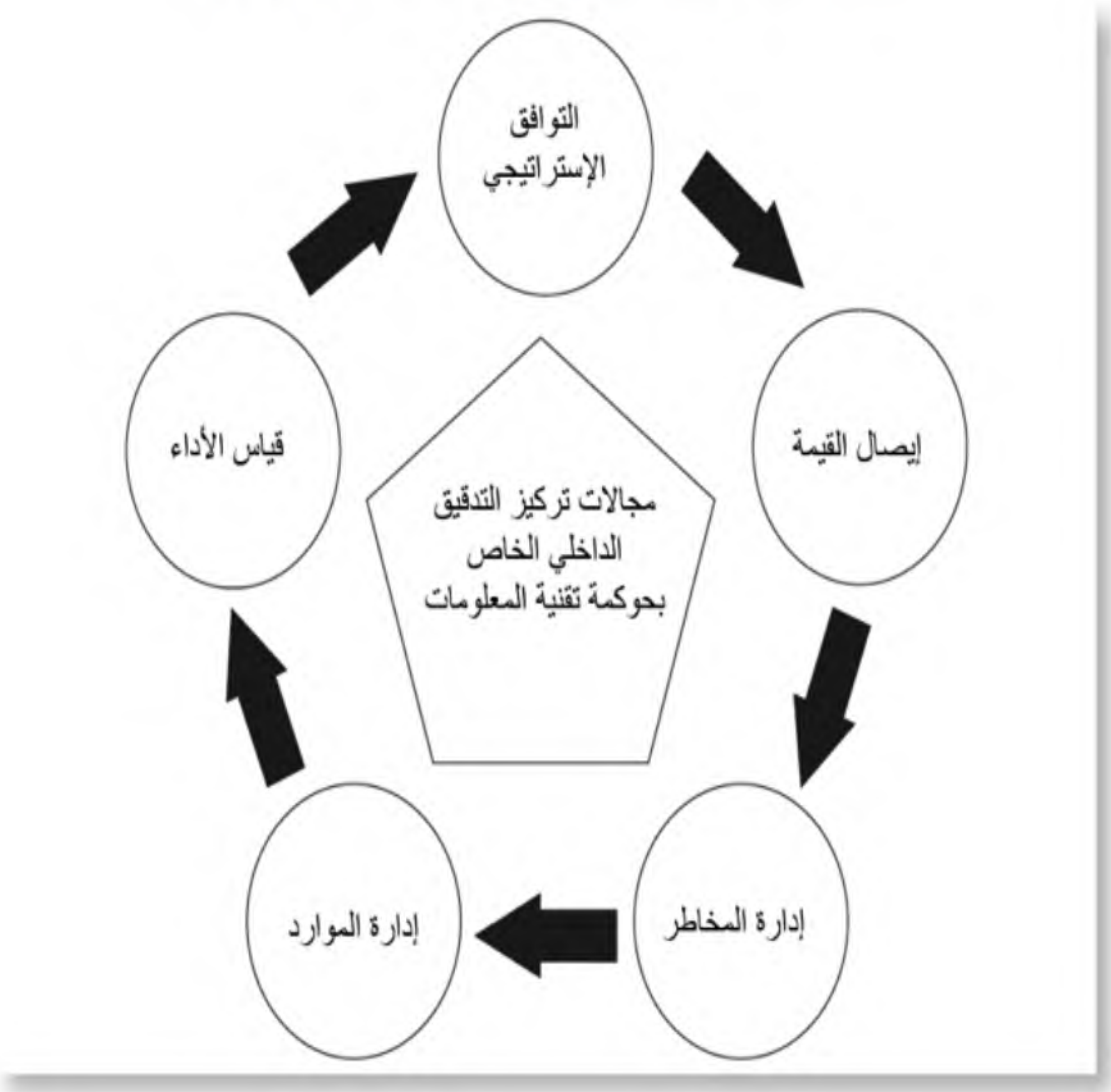
استناداً إلى حديثنا في الفصول السابقة عن حوكمة تقنية المعلومات، فإن الأهداف الرئيسية لحوكمة تقنية المعلومات هي التأكد من أن الاستثمارات في تقنية المعلومات تُوجِد قيمة للأعمال، وتخفف من المخاطر المرتبطة بعمليات ونظم تقنية المعلومات. يمكن للعديد من الأنشطة الخاصة بمراجعات عمليات التدقيق الداخلي أن تلعب دوراً رئيسياً في دعم حوكمة تقنية المعلومات في المؤسسة. مثال على ذلك، نشاط التدقيق الداخلي المستمر لتقنية المعلومات عبارة عن مراجعات وتقييمات للخطط الخاصة باستمرارية تقنية المعلومات المؤسسية، التي كانت تسمى في فترة من الفترات خطط التعافي من كوارث تقنية المعلومات في زمن نظم الحاسبات المركزية. وإن إدارة تقنية المعلومات في المؤسسة تحتاج إلى عمليات معمول بها لاستعادة العمليات التشغيلية والموارد الخاصة بتقنية المعلومات وإعادتها إلى مستوياتها التشغيلية الطبيعية في حال حدوث عطل ما طويل الأجل في خدمات تقنية المعلومات. إن مراجعات وتقييمات التدقيق الداخلي في هذا المجال تدعم إلى حد كبير عمليات حوكمة تقنية المعلومات في المؤسسة.

وقد تدعم عمليات التدقيق الداخلي إلى حد كبير العمليات الخاصة بحوكمة تقنية المعلومات المؤسسية من خلال إجراء المراجعات والتقييمات في هذه المجالات العامة. الشكل التوضيحي (١٩-٤) يحدد خمسة مجالات عامة يجب أن يركز عليها التدقيق الداخلي أثناء مراجعاته لحوكمة تقنية المعلومات: إيصال القيمة وإدارة المخاطر والموارد والأداء وقضايا التوافق الإستراتيجي. إن المعايير المهنية للتدقيق الداخلي تتطلب المستويات التالية من أنشطة أعمال المراجعة لعملية التدقيق الداخلي:

- مراجعة وتقييم عملية إيصال القيمة المرجوة من إدارة تقنية المعلومات، وكيف تتماشى تقنية المعلومات مع رسالة ورؤية وقيم وأهداف وإستراتيجيات المنظمة.
- مراجعة ما إذا كان لدى إدارة تقنية المعلومات بيان واضح عن الأداء المتوقع للعمل (من حيث الفاعلية والكفاءة) وتقييم مدى إنجازه.
- مراجعة وتقييم فاعلية عمليات إدارة موارد تقنية المعلومات وأدائها.

شكل توضيحي (١٩-٤)

مجالات تركيز التدقيق الداخلي لحوكمة تقنية المعلومات



- مراجعة وتقييم التوافق مع المتطلبات القانونية والبيئية ومتطلبات جودة المعلومات والمتطلبات الائتمانية والأمنية.
- مراجعة وتقييم البيئة الرقابية للمنظمة.
- مراجعة وتقييم المخاطر التي قد تؤثر سلباً في بيئة تقنية المعلومات.

يجب أن يـدرك ويعترف المديرون التنفيذيون للأعمال غير المشـاركين في مهام التدقيق الداخلي بأن إدارة التدقيق الداخلي هي كيان مسـتقل في المؤسسـة، ولا يستطيع أي مدير تنفيذي من خارج لجنة التدقيق أن يقوم بإعطاء توجيهات لعملية التدقيق الداخلي للقيام بإجـراء مراجعات في منطقة ما. وأن خطـط مراجعة التدقيق الداخلي الخاصة بهم ينبغي ألا يتم وضعها إلا من خلال موافقة لجنة التدقيق. ومع ذلك، ينبغي أن يشـعر الموظفون التنفيذيون للعمليات التشـغيلية في المؤسسـة أو إدارة تقنية المعلومات بأن لديهم مطلق الحريـة في أن يسـألوا الرئيس التنفيذي للتدقيق وغيره من أعضـاء إدارة التدقيق الداخلي عـن خططهم وأنشـطتهم الحالية في مراجعة النواحي الرئيسـية التي تخص حوكمة تقنية المعلومات في المؤسسة.

مراجعات التدقيق الداخلي لعمليات التوافق الإستراتيجي لتقنية المعلومات:

ومن ضمن الخطط السـنوية والأنشطة الجارية لإدارة تقنية المعلومات في المؤسسة، أنه يجب على التدقيق الداخلي القيام بتقييم ما إذا كانت تلك الخطط والعمليات التشـغيلية الخاصة بتقنية المعلومات تنسجم مع أنشطة الأعمال الأخرى في المؤسسة. العنصر الرئيسي لتحقيق ذلك هو أنه يجب على جميع العمليات التشغيلية لتقنية المعلومات، متضمناً ذلك تطوير النظم وإدارة الجودة ومعالجة تقنية المعلومات أن تنسجم مع العمليات التشغيلية للأعـمال. بمعنى أنه يجب أن يكون للعمليات التشـغيلية لتقنية المعلومات قيمة وموقع تنافسي في المنتجات والخدمات التي تقدمها المؤسسـة. إن إدارة تقنية المعلومات يجب أن تسـعى جاهدة للحفاظ على تكاليفها من خلال تحسـين الكفاءة والفاعلية الإدارية. وعلى الرغم من أن هذه الأمور تمثل كل النداءات الخاصة بإدارة تقنية المعلومات والإدارة العامة، فإنه يجب دائماً على إدارة التدقيق الداخلي القيام بطرح بعض الأسئلة الصعبة أثناء قيامها بمراجعة أنشطة الأعمال.

كما ذكرنا سـابقاً، فإن الإدارة الفعالة لتقنيـة المعلومات ينبغي أن يكون لديها نوع من أنـواع اللجان التوجيهية، التي تقوم بمهمة التخطيـط الطويل الأجل حيث يمكن أن يلتقي مزيج متنوع من مسـتخدمي مـوارد تقنية المعلومات مع إدارة تقنيـة المعلومات ليقوموا بمراجعة أو الموافقة على المقترحات الجديدة وتحديد الأولويات المتعلقة بالأعمال الجديدة.

يجــب على عمليات تدقيق تقنية المعلومات أن توصي وتشــدد على وجود وجاهزية هذه الإدارة الفعالة، كما يجب أن تشارك في أغلب الاجتماعات التي تجريها تلك اللجنة التوجيهية. ويجب أن تقوم اللجنة التوجيهية بوضع إســتراتيجية بعيدة المدى لأنشــطة واســتثمارات تقنية المعلومات والمراجعات الدورية للتدقيق الداخلي، من خلال المشــاركة غير الفعالة في جلسات اللجنة التوجيهية أو المراجعات الرسمية للتدقيق الداخلي، وينبغي تأكيد أن تكون هذه الإستراتيجية لتقنية المعلومات في موضوع التنفيذ وجاهزة للعمل.

لا بد من وجود نهج متكامل لعمل المؤسســة وإستراتيجية تقنية المعلومات، ومهام ذات مســؤولية تشاركية بينهما. وبالإضافة إلى ذلك، وعلى الرغم من أن إدارات تقنية المعلومات تكــون ملامــة أحياناً على تبنيها لأســاليب جديدة وغير مجربة، فإنه يجــب أن يكون هناك تصريح واضح بأهداف تلك الأســاليب المتبعة. وقد تمثل عملية التدقيق الداخلي من خلال مراجعاتها وتعليقاتها التدقيقية الصوت الفعال للمساعدة في ضمان تحقيق هذه الأهداف.

مراجعات التدقيق الداخلي لعمليات إيصال قيمة تقنية المعلومات:

يجــب أن تكون مراجعــات التدقيق الداخــلي مصممة لضمان اســتمرار تقديم تقنية المعلومات لفوائدها المرجوة وفق إســتراتيجياتها المعلنة. إن الفكرة هنا هي أن المشــاريع الجديــدة لتقنية المعلومات، ســواء كانت عمليات تطبيقية جديدة أو محســنة أم أدوات ومعــدات جديدة يتــم اقتراحها للحصول عــلى الفوائد المتوقعة. ومع أنــه من المؤكد أن عملية التدقيق الداخلي لن تكون قادرة على مراجعة جميع هذه الأعمال، نتيجة الأولويات المفروضة ومحدودية الموارد، فإنه يجب القيام بعملية تقييم دوري للفوائد المعلنة لاكتشاف مــا إذا كانت الأهــداف المعلنة قد تم تحقيقهــا بالفعل أم لا. ينبغــي أن يبحث التدقيق الداخلي عن عوائد الاستثمار الرســمية، والتكلفة الإجمالية للملكية، ووسائل لقياس أعمال تقنية المعلومات.

وكــما تحدثنا في الفصل الســادس عشر من هذا الكتاب عــن موضوع إدارة المشروعات، فإن إدارة تقنية المعلومات المؤسســية ينبغي أن يكون لديها عملية رســمية متعارف عليها ومعمول بها لإدارة مشاريع تقنية المعلومات لإيصال الفوائد إلى العمليات التشغيلية للأعمال. إن تقييــم إيصال القيمة يتجاوز كثيراً العمليــات التقليدية للتدقيق الداخلي التي تركز على

الضوابط الداخلية، ويتطلع لإيصال قيمة أفضل للعمليات التشغيلية لتقنية المعلومات. كما أن هناك حاجة إلى التزام رسـمي لوضع منهجيات رسـمية للتطوير الشـامل لعملية تقديم خدمات تقنية المعلومات.

إن هـذا المفهوم لمراجعـات التدقيق الداخـلي الخاصة بعمليات تقديـم خدمات تقنية المعلومـات يتجاوز الكثير من الجهود المبذولة في المراجعات الاعتيادية للتدقيق الداخلي. وقد ناقش الفصل السادس من هذا الكتاب موضوع تقديم خدمات تقنية المعلومات على أنه جزء من المفاهيم الخاصة بالإطار آيتل وإدارة خدمات تقنية المعلومات. إن الإدارة الفعالة للتدقيق الداخلي تحتاج لاستيعاب هذه المفاهيم ومزجها مع الإجراءات الأخرى للتدقيق الداخلي.

مراجعات التدقيق الداخلي لعمليات إدارة مخاطر تقنية المعلومات:

كما أكدنا في الفصل الثامن من هذا الكتاب الذي يدور حول إدارة المخاطر وفي الشروحات الأخـرى طوال هذه الفصول؛ فـإن إدارة المخاطر تعد مفهوماً مهماً جداً بالنسـبة لحوكمة تقنية المعلومات، وأن فهمها ووضعها محل التقدير ينبغي أن يكون بالفعل جزءاً من جميع مراجعات التدقيق الداخلي. وهذا يتطلب توعية من كبار المسؤولين عن الرغبة في المخاطر الخاصة بالمؤسسـة. لذا يجب تضمين مسـؤوليات إدارة مخاطر تقنية المعلومات في جميع مستويات العمليات التشغيلية للأعمال. وهذا المجال يهتم غالباً بعمليات تقنية المعلومات حيث كانت هناك ميول تاريخية لتجربة أساليب جديدة للنظم أو التقنيات مع القليل من الفهـم لأي مخاطر مرتبطـة بها. وعلى الرغم من أن إدارة تقنية المعلومات ومسـتخدمي تقنية المعلومات ينبغي أن يكونوا هم المسؤولين في هذه الحالة، فإنه يكون هناك غالباً ميل لتجربة بعض الأسـاليب الجديدة وغير المجربة مع قليل من التفكير في المخاطر إذا فشلت. ويمكن للتدقيق الداخلي في كثير من الأحيان أن يكون فعالاً جداً من خلال أخذ دور محامي الشيطان في طرح الأسئلة الصعبة بوصفها جزءاً من مراجعاتها.

إن العمليات المناسبة لإدارة المخاطر ينبغي أن تركز على حماية أصول تقنية المعلومات ودعم النظم من خلال إجراءات التعافي من الكوارث والخطط الفعالة لاستمرارية العمليات التشـغيلية. لقد كان هذا هو المجال التقليـدي لمراجعات التدقيق الداخلي وتدقيق تقنية المعلومات، وينبغي تأكيدها على أنها جزء من أنشطة مراجعة حوكمة تقنية المعلومات.

ينبغي أن تركز جميع مراجعات التدقيق الداخلي على التوعية بمخاطر تقنية المعلومات على أســاس من الشفافية لجميع أصحاب المصالح، ولا بد من بذل الجهود من أجل تضمين إدارة المخاطر باعتبارها جزءاً متمماً لامتثال وضمان المؤسســة. وينص ذلك حقيقة على أن إدارة التدقيــق الداخلي يجب أن تذهب إلى ما هو أبعــد من مجرد المراجعات المتخصصة لتدقيق تقنية المعلومات وإضافة مخاوف إدارة مخاطر تقنية المعلومات لجميع المراجعات التــي تغطي مجالات حوكمة تقنية المعلومات. وبالإضافة إلى العمليات الشــاملة للتدقيق الداخــلي، فــإن هناك حاجة إلى إنشــاء تقييمات فعالــة لإدارة العملية عــلى أنها جزء من مراجعات التدقيق الداخلي.

مراجعات التدقيق الداخلي لعمليات إدارة موارد تقنية المعلومات:

يتعين عــلى التدقيق الداخلي لتقنية المعلومات أن يراجع ويقيم بانتظام فاعلية عملياته الخاصة بإدارة موارد تقنية المعلومات وأدائها. ففي العديد من المؤسسات، تعد مرافق تقنية المعلومات وعملياتها التشــغيلية إحدى الاحتياجات الرئيســية فيها - إن لم تكن الرئيسية - لموارد المؤسســة. وينبغي على الإدارة أن تســتثمر في هذه الموارد الخاصة بتقنية المعلومات من خلال خطط رســمية لمشروعات طويلــة المدى والعمليات المتبعــة في وضع الميزانيات. وقد قامت الفصول الأخرى بتغطية مسائل تتعلق بإدارة موارد تقنية المعلومات من منظور عمليات التشــغيل الشــاملة. على ســبيل المثال، الفصل الرابع عشر من هذا الكتاب ناقش أهميــة إدارة محافظ وتهيئة تقنية المعلومات لتكون وســيلة لإدارة وضبط الأصول المتنوعة لتقنية المعلومات بشكل أفضل. وكذلك ناقش الفصل السابع عشر من هذا الكتاب اتفاقيات مستوى الخدمة ليكون وسيلة لتعظيم قيمة استثمارات الأعمال.

يجب على التدقيق الداخلي أن يخطط ويطور سلســلة من المراجعات في هذه المجالات الخاصــة بإدارة موارد تقنية المعلومات. وفحوى ذلك أنــه من الصعب على إدارة التدقيق الداخلي مجرد إطلاق مراجعة لإدارة موارد تقنية المعلومات، عندما يكون الموضوع والمجال تقريباً واســعاً جــداً لمراجعة واحدة للتدقيــق الداخلي. بل يجب عــلى التدقيق الداخلي أن يطــور وينفذ مراجعــات متخصصة في العديد إن لم يكن جميــع مجالات حوكمة تقنية المعلومات التي تمت مناقشتها في هذه الفصول.

مراجعات التدقيق الداخلي لعمليات قياس أداء تقنية المعلومات:

يجــب تطوير تقنيات لقياس الأداء للمســاعدة في ترجمة الإســتراتيجيات إلى أفعال مــن أجــل تحقيق وقياس إنجازات أهــداف تقنية المعلومات. هــذا النوع من الأدوات يمكــن أن يقيس العلاقات والأصول اللازمة لتحقيق التركيز على العميل وكفاءات العملية والتســهيلات لمســاعدة المؤسســة وإدارات تقنية المعلومات الخاصة بها بشــكل كلي في التعلم والنمو. هذه الأنواع من الأدوات تتبع عملية تقديم المشــاريع ومتابعة خدمات تقنية المعلومات.

الشكل التوضيحي (١٩-٥) يوضح أنواع أنشطة مراجعة وتقييم التدقيق الداخلي اللازمة لتعزيز حوكمة تقنية المعلومات في المؤسســة. إن هذا الشكل على مستوى عال جدا ولكن يؤكــد أن المدققــين الداخليين بحاجة إلى مراجعة نظم وعمليات تشــغيل تقنية المعلومات للمساعدة في تحسين العمليات الشاملة للرقابة الداخلية للمؤسسة وتبسيط وتحسين هذه العمليــات ورفع توصية بمجالات معينة لأتمتتها بشــكل أفضل، واقــتراح مجالات يتم عمل توحيد قياسي لعملياتها ونظمها بشكل أفضل.

إن مجالات مراجعة التدقيق الداخلي هذه تغطي مجموعة واسعة من أنشطة التدقيق التي تتجاوز شروحات التدقيق الداخلي السابق تلخيصها في هذا الفصل والتي تعد جزءاً من أفضل ممارســات التدقيق الداخلي الشائعة لاحتياجات المعرفة. إن الإدارة الفعالة للتدقيق الداخلي ينبغي أن تكون عنصراً رئيسياً في تعزيز العمليات الفعالة لحوكمة تقنية المعلومات في أي مؤسسة.

شكل توضيحي (١٩-٥)

أنشطة مراجعة التدقيق الداخلي لحوكمة تقنية المعلومات



ملاحظة:

١. الآن في طبعته السابعة، Brink's Modern Internal Auditing تم نشره من خلال جون وايلي واولاده، عن طريق روبرت ر. مولر كمؤلف.

الجزء السادس
حوكمة تقنية المعلومات وأهداف المؤسسة

الفصل العشرون
بناء ثقافة أخلاقية في محل العمل والحفاظ عليها

كما تحدثنا في الفصول السابقة، فإنه لا بد من دمج عمليات حوكمة تقنية المعلومات مع عمليات التشغيل الأساسية لأعمال المؤسسة ويجب أيضاً أن تقع مسؤولية ضمان العمليات الصحيحة لحوكمة تقنية المعلومات على عاتق إدارة كل وحدة تابعة أو وحدة أعمال في المؤسسة أينما كانت. وباعتبار المؤسسة أحد العناصر الأساسية في هذا الصدد، فإنه يجب عليها أن تلتزم بتحقيق أعلى معايير الأخلاق والنزاهة في جميع مجالات عملياتها التشغيلية. يجب أن تبدأ نزاهة المؤسسة بالتزام كل أصحاب المصلحة وكل موظف بالقيم الأساسية للمؤسسة وبمسؤوليته لأداء دوره بالشكل الذي يتوافق مع تلك القيم ويخدمها.

يناقش هذا الفصل أهمية أخلاقيات العمل، وسياسات الحوكمة في المؤسسة، وهياكل الإشراف والعمليات، والخطوات اللازمة لإنشاء إدارة فعالة لأخلاقيات العمل، ووضع وتطبيق قوانين فعالة للسلوك، وإنشاء لجنة فعالة لامتثال المؤسسة تحت رئاسة مجلس الإدارة. إن هدفنا هو ذكر بعض أفضل الممارسات التي يمكن للمؤسسة اتباعها وتطبيقها لإرساء ثقافة أخلاقية في مكان العمل.

لا تقتصر القضايا وأفضل الممارسات المذكورة في هذا الفصل على عمليات تشغيل تقنية المعلومات وحوكمة تقنية المعلومات بل تمتد لتشمل جميع جوانب المؤسسة. ومع ذلك، فإن أفضل الممارسات مثل مدونة قواعد السلوك الفعالة للمؤسسة وبيان المهمة (الرسالة) المدعومة من الإدارة العليا ينبغي أن تحصل على الدعم من جميع أصحاب المصلحة في المؤسسة. ويجب أن تكون النتيجة النهائية هي بناء الثقافة الأخلاقية في مكان العمل.

أهمية بيانات المهمة (الرسالة):

لقد ناقشت الفصول السابقة من هذا الكتاب العديد من القضايا الهامة في حوكمة تقنية المعلومات، وركز معظمها على الحاجة إلى وضع معايير وعمليات فعالة لحوكمة تقنية المعلومات، مثل الفصل السابع من هذا الكتاب المتعلق بمعايير الأيزو الخاصة بالحوكمة،

أو الفصل الثاني عشر من هذا الكتاب أيضاً الخاص ببيان خدمات عمليات تشغيل تقنية المعلومات. إذ يركز كل فصل من هذه الفصول على مجالات محددة لتحسين عمليات تشغيل تقنية المعلومات في المؤسسة. في جميع الأحوال، فإن البيان الفعال لمهمة أو رسالة المؤسسة، والذي يغطي كل جوانب عمليات التشغيل وجميع أصحاب المصلحة، ينبغي أن يكون عنصراً أساسياً في إرساء ممارسات فعالة لحوكمة تقنية المعلومات.

تحتاج كل مؤسسة بغض النظر عن حجمها إلى بيان مهمة أو رسالة لوصف جميع أهدافها وقيمها. وينبغي أن تكون تلك الرسالة بمثابة مصدر للتوجيه - بوصلة - تسمح للموظفين والعملاء والمساهمين وغيرهم من أصحاب المصلحة بمعرفة ما تمثله المؤسسة وما لا تمثله. لقد كان بيان الرسالة في السنوات الماضية في كثير من الأحيان أكثر بقليل من مجرد شعار لطيف لكنه يبدو مُرهقاً، أما اليوم فيجب أن يكون البيان الفعال لرسالة المؤسسة عنصراً مهماً جداً في أي برنامج لأخلاقيات الإدارة والحوكمة الرشيدة للشركات. قد يكون البيان الفعال للرسالة أحد الأصول العظيمة للمؤسسة والذي يسمح لها بتحقيق جميع أهدافها وأغراضها على نحو أفضل.

على الرغم من مرور سنين طويلة على أزمة جونسون أند جونسون تايلينول Johnson & Johnson Tylenol التي وقعت أوائل ثمانينيات القرن الماضي، فإنها لا تزال تقدم مثالاً جيداً على أهمية البيان القوي لمهمة أو رسالة المؤسسة والذي يعمل كبوصلة لتقديم التوجيه المناسب. تعد شركة جونسون آند جونسون، واحدة من كبار موردي المنتجات الطبية، حيث قامت بتصنيع دواء شائع مسكن للألم ويؤخذ بدون وصفة طبية يسمى تايلينول Tylenol. وقد كانت هذه الأدوية تباع وقتها في زجاجات تغلق من الأعلى بسدادة لولبية. وقد قام أحد الأشخاص القاطنين في منطقة شيكاغو بفتح عدة زجاجات من دواء تايلينول هذا، وقام بغش محتوياتها بإضافة مادة السيانيد إليها، وقام بوضع هذه الزجاجات محل زجاجات أخرى على رفوف المتجر. وقد توفي العديد من الأشخاص الذين قاموا بشراء هذا التايلينول الملوث في وقت لاحق نتيجة تعرضهم للتسمم. وقد أشارت التحقيقات التي أُجريت على هذه الحالات بسرعة إلى جونسون آند جونسون والتايلينول الملوث بالسيانيد.

هــذا الأمر برمته قد وضع شركة جونســون آند جونســون تحت وطـأة ضغوط هائلة. فقــد كانت الشركة تعلم تماماً أنهــا تمتلك عمليات قوية جداً ومعمــولاً بها لضبط الجودة التي من شــأنها أن تمنع حدوث مثل هذا التلوث الســام داخل مرافق التصنيع الخاصة بها. وعلمت أيضاً أن المنتجات الملوثة قد ظهرت فقط في منطقة شــيكاغو، في حين أن تايلينول كان موجــوداً عــلى رفوف المتاجر في جميع أنحاء العالم. إن عملية الســحب الكلي للمنتج ستكون مكلفة للغاية. ومع ذلك، فإن شركة جونسون آند جونسون لم تقم بسلسلة طويلة مــن التحقيقات الداخلية وقد قامت بسرعة باتخاذ الإجراء الصحيح. وقامت بســحب كل منتجــات تايلينــول الخاصة بها من رفوف المتاجر في جميع أنحــاء العالم، وبعد ذلك قامت بإعادة إصدارها لهم في عبوات مختومة بتصميم جديد. وعندما سُئلت الشركة لماذا قامت بإصدار مثل هذا القرار بسرعة والخاص بســحب المنتج بالكامــل رغم تكلفته العالية جداً ورغــم عدم وجود دليل على أنها كانت عــلى خطأ، أفادت الشركة بأنه لم تكن هناك حاجة لتأخير القرار. إن توجه شركة جونســون آند جونسون ورسالتها قد أملت عليها ذلك القرار. إن توجه جونســون آند جونسون ينص وبشــدة على أن المسؤولية الأولى للشركة هي توفير منتجــات عالية الجــودة لعملائها. ويمكن العثور على نص هــذا التوجه على موقع الويب الخاص بشركة جونســون آند جونسون وهي مبينة في الشكل التوضيحي (٢٠-١). في وقت أزمة التايلينول، كان الجميع في شركة جونسون آند جونسون على علم بهذا التوجه، فقد تم نشر هذه التوجه على نطاق واســع في مرافق المؤسســة، ولم يكن هناك حاجة وقتها لاتخاذ قرار بذلك. إن هذا الأمر المؤســف برمته قد أبرز بالفعل أهمية وجود بيان قوي لمهمة أو رسالة المؤسسة.

يعد البيان القوي لرســالة الشركة عنــصراً هاماً في أي مبادرة مــن مبادرات الأخلاقيات وحوكمــة الــشركات. وعلى الرغم من أن معظم الشركات لن تواجه أزمة في مســتوى أزمة شركة جونســون آند جونســون مع تايلينول الملوث التي حدثت في ثمانينيات القرن الماضي، فإن قواعد قوية من هذا النوع قد ســاعدت بعض الشركات لتجنب الفضائح المحاســبية في الســنوات الأخيرة بصورة أفضل، تلك الفضائح التي أدت إلى ظهور قانون ســاربينز أوكسلي (SOx) كما وضحنا في الفصل الثاني من هذا الكتاب.

شكل توضيحي (٢٠-١)

توجه أو بيان مهمة جونسون آند جونسون

توجهنا (كما نشرت في JnJ.com)

نحن نؤمن أن مسـؤوليتنا الأولى هـم الأطباء والممرضات والمرضى حتى الأمهـات والآباء والجميع غيرهم ممن يسـتخدمون منتجاتنا وخدماتنا. وفي سبيل تلبية احتياجاتهم فإن كل شيء نقوم به يجب أن يكون ذا جودة عالية. ويجب أن نسعى جاهدين وبصفة مستمرة لخفض تكاليفنا من أجل الحفاظ على أسـعار معقولة. إن طلبـات العملاء يجب تلبيتها بسرعة وبدقة، ويجـب أن يكون لدى موردينا وموزعينا فرصة لتحقيق ربح عادل.

نحن مسـؤولون عن موظفينا، الرجال والنسـاء الذين يعملون معنا في جميع أنحاء العالم. يجب أن يُنظر إلى كل فرد كإنسـان، ويجب علينا احترام كرامتهم والاعتراف بفضلهم. يجب أن يكون لديهم شـعور بالأمن في وظائفهم، والتعويض يجب أن يكون عادلاً ومناسـباً، أجـواء العمل نظيفة، ومنظمة وآمنة. يجب علينا أن نفكر في طرق لمسـاعدة موظفينا حتى يسـتطيعوا الوفاء بمسؤولياتهم الأسرية. يجب أن يشـعر الموظفون أنهم أحرار في تقديم الاقتراحات والشـكاوى. يجب أن يكون هناك تكافؤ فـرص للعمل والتنميـة والتقدم لأولئك المؤهلين. يجـب أن نوفر الإدارة المختصـة، ويجب أن تكون تصرفاتهم عادلة وأخلاقية.

نحـن مسـؤولون عن المجتمعات التي نعيش ونعمل فيها والمجتمـع الدولي أيضاً. يجب أن نكون مواطنـين صالحين - ندعم الأعمال الصالحة والجمعيـات الخيرية ونتحمل نصيبنا العادل من الضرائب. يجب علينا أن نشـجع التحسينات المدنية وتحسـين الصحة والتعليم، ويجب أن نُبقي على الممتلكات المصرح لنا باستخدامها في حالة جيدة، نحمي البيئة والموارد الطبيعية.

مسـؤوليتنا النهائيـة تكون تجاه أصحـاب المصلحة لدينا. العمل يجب أن يجني ربحاً سـليماً. لا بـد لنا مـن تجربة أفكار جديدة. يجب أن يتم إجراء البحوث بشـأن ابتكار برامج متطورة ودفع ثمن الأخطاء. يجب شراء المعدات الجديدة وإطلاق الوسـائل الجديدة المتوفرة والمنتجات الجديدة. يجب إنشـاء الاحتياطيات لتغطية أوقات العسر. عندما نعمل وفقاً لهذه المبادئ، ينبغي أن يحقق أصحاب المصلحة عائداً عادلاً.

المصدر: جونسون آند جونسون.

يتعين على إدارة المؤسســة القيام بتقييم أي بيان ممكن أن يكون موجوداً اليوم لرسالة المؤسسة أو النظر في صياغته وإطلاق بيان آخر جديد إذا لزم الأمر. وإذا كان هناك موظفون أو غيرهم من أصحاب المصلحة ليســوا على علم بوجود أي بيان خاص بمهمة الشركة أو إذا كانــوا ينظرون إليه بشيء من الســخرية، فإن هناك حاجة إلى إعــادة النظر في تلك الوثيقة ومراجعتها. تجد غالباً أن الضرر الناتج عن بيان الرســالة السيء الصياغة يتجاوز نفعه، بل ويــؤدي إلى ظهور أعضــاء في المنظمة ممن يقاومون التغيير يعبرون عن ســخريتهم وعدم سعادتهم حيال ذلك. إذا لم يكن لدى المؤسسة أي بيان للمهمة أو القيم، فقد يكون هناك قيمة كبيرة في تكوين فريق يقوم بوضع بيان يعكس القيم والمقاصد العامة للمؤسسة. إذا تعرض البيان الحالي لمهمة المؤسســة إلى التهكم أو السخرية من خلال استبيانات استقصاء آراء أصحــاب المصالح، إذاً فقد حان الوقت لصياغــة وتنقيح هذا البيان بعناية. من ناحية أخــرى، إذا تم تعميمه دون أي تحضيرات، فمن الممكــن أن يُنظر إليه بالمزيد من التهكم. يعد البيان الجيد لمهمة المؤســة أيضاً بمثابة نقطة انطلاق جيدة لرسالة "النغمة السائدة" لشركات اليوم، كما سبق مناقشته في الفصل الثاني من هذا الكتاب.

إن البيــان الجيد لمهمة المؤســة يجب أن يؤدي إلى تقاريــر إيجابية عن الشركة. كما ينبغــي أن يلهم وبكل أمل أعضاء المنظمة لتســخير طاقاتهم وحماســهم وزيادة التزامهم لتحقيق الأهداف والغايات. إن الفكرة الأساسية هي إيجاد الشعور بالهدف والاتجاه الذي سوف تتم مشاركته في جميع أنحاء المؤسسة. وبالعودة مرة أخرى بالزمن قبل عدة سنوات، فقــد يكــون أحد أفضل الأمثلة على بيان المهمة هو ما عــبر عنه الرئيس الأمريكي جون ف. كينيدي John F. Kennedy في أوائل ستينيات القرن الماضي:

> "يتوجــب على هذه الأمة أن تتفرغ تماماً لتحقيق الهدف، قبــل انقضاء هذا العقد، بهبوط الإنسان على القمر وعودته إلى الأرض سالماً".

فقد قامت تلك الكلمات البسيطة بوصف المهمة والرؤية أفضل بكثير من وثيقة ضخمة تحتوي على العديد من الصفحات. وهي تسمى أحياناً بيانات القيم أو العقائد (التوجهات)، ويمكن أيضاً العثور على تلك البيانات في التقارير الســنوية للعديد من المؤسســات. بعضها طويــل، والبعض الآخر يبدو قصيراً بدرجــة ملحوظة. فالبيان الأفضل هو ذلك الذي يُكتب

بأسـلوب قريب من صياغة التوجه الخاص بجونسـون آند جونسـون أو بيان الهبوط على سطح القمر وفق أسلوب صياغتهم.

بمجـرد أن تقوم المؤسسـة بوضع بيان جديد للمهمة أو الرسـالة أو تقـوم بتنقيح بيان مهمة موجود، فإنه يجب تعميمه على كل أعضاء المؤسسـة مع مسـتوى جيد من الدعاية. ومن خلال اسـتخدام نهـج النغمة السـائدة، فإنه يتعين على كبار المديرين شرح أسـباب البيان الجديد للمهمة ومدى أهميته بالنسـبة للمؤسسة. ويجب نشره في لوحات إعلانات المؤسسـة وفي التقرير السنوي وفي غيرها من الأماكن لتشجيع جميع أصحاب المصلحة على فهمـه وقبوله. يجب ألا يعمل بيان المهمة بشـكل منفصل، فهناك حاجة إلى سلسـلة من الخطـوات الأساسـية الأخرى لبناء إدارة فعالـة للامتثال والأخلاقيات، بدءاً من الدراسـات الاستقصائية وغيرها من الآليات.

مدونة قواعد السلوك للمؤسسة:

في الوقت الذي يُعد فيه البيان القوي والفعال لمهمة الشركة عنصراً أساسياً في الهيكل العام لحوكمة الشركات، تعمل مدونة قواعد السـلوك على توفـير قواعد الدعم اللازمة لأصحاب المصلحة في المؤسسـة. لقد كانت هذه القواعد شائعة في الشركات الكبرى لسنوات عديدة، ويطالب قانون SOx اليوم الشركات بوضع مدونة أخلاقيات لكبار المسـؤولين الماليين. وبما أنه قد تم فرض هذه المدونة من قبل قانون SOx، فبإمكان جميع الشركات أن تستفيد من مدونة قواعد السلوك التي تشمل جميع أصحاب المصلحة. وعلى الرغم من أن قانون SOx يسـتخدم تعبير "مدونة أخلاقيات المهنة"، فإننا نشـير إليها هنا باسمها الذي قد يكون أكثر شيوعاً وهو مدونة قواعد السلوك المهني للمؤسسة.

يجب على المؤسسة اليوم أن تضع وتطبق مدونة لقواعد السلوك المهني تشمل مجموعة مناسـبة من القواعد الأخلاقية وقواعد العمل والقواعـد القانونية لجميع أصحاب المصالح في المؤسسـة، متضمناً ذلك الإدارة العليا وجميـع العاملين والمشرفين وأكبر فئة من أصحاب المصلحـة بهـا. يجب أن تقـوم الإدارة العليا للمؤسسـة بتكوين فريق مكـون من أعضاء العمليات التشـغيلية للوحـدات والمديرين الماليين وممثلين عن الرقابـة الداخلية وضمان الجودة واتصالات الشركة والموارد البشرية وبالتأكيد الإدارة القانونية للشركة، وذلك لبناء أو

إعادة بناء مدونة فعالة لقواعد السلوك المهني والتي تُشجع الممارسات الأخلاقية للأعمال في جميع أنحاء المؤسسة.

المحتويات: ماذا يجب أن تكون رسالة المدونة؟

ينبغي أن تكون مدونة قواعد السلوك عبارة عن مجموعة من القواعد أو التوجيهات الواضحة التي لا لبس فيها ولا غموض والتي تحدد ما هو متوقع من أعضاء المؤسسة، سواء كان المتوقع من المسؤولين أم من الموظفين أو المقاولين أو البائعين أو أي من أصحاب المصالح الآخرين. وينبغي أن تستند المدونة إلى القيم والقضايا القانونية المحيطة بالمؤسسة. بمعنى أنه على الرغم من أن جميع المؤسسات يُفتَرَض تبنيها لمدونة قواعد السلوك المهني بما فيها محظورات ضد التمييز الجنسي والعنصري، فإننا نجد أن مقاول الدفاع(*) الذي يكون لديه العديد من القضايا المرتبطة بالقواعد المتعلقة بالتعاقدات سيحتفظ لديه بمدونة قواعد سلوك مهني مختلفة نوعاً ما عن تلك الخاصة بعملية تقديم الوجبات السريعة. ومع ذلك، يجب تطبيق أي مدونة بهذا الشكل على جميع أعضاء المؤسسة من أعلى مستوى وحتى موظف الأعمال الكتابية الذي يعمل بدوام جزئي. فعلى سبيل المثال، فإن مدونة قواعد السلوك التي تمنع رفع تقارير مالية خاطئة يلزم أن تكون هي المدونة نفسها، سواء تم توجيهها إلى المدير المالي فيما يخص التقارير المالية الخاطئة أم إلى الموظف الذي يعمل بدوام جزئي فيما يخص بطاقة الدوام الأسبوعي غير الصحيحة أو الاحتيالية.

إذا كانت المؤسسة لديها بالفعل مدونة لقواعد السلوك، فإنه ينبغي على إدارة المؤسسة النظر في تنقيحها أو تحديثها بحسب الحاجة. في كثير من الأحيان، نجد أنه تم وضع المدونات القديمة لتكون بالأساس قواعد لموظفي المستوى الأدنى، مع القليل من الاهتمام

(*) يسمى أيضاً المقاول الأمني (security contractor) وهي منظمة تجارية أو فرد يقدم منتجات أو خدمات لإدارة عسكرية أو استخباراتية تابعة للحكومة. وتشمل المنتجات عادة الطائرات العسكرية أو المدنية، والسفن، والمركبات، والأسلحة، والأنظمة الإلكترونية. ويمكن أن تشمل الخدمات اللوجستية والدعم التقني والتدريب ودعم الاتصالات والدعم الهندسي بالتعاون مع الحكومة. (المترجم).

الموجه للعديد من كبار أعضاء المؤسســة. إن المدونة الفعالة لقواعد السلوك المهني ينبغي توصيلها بطريقة من شــأنها أن تُطَبَق على جميع أصحاب المصلحة في المؤسســة، مع تركيز أكـثر اليوم على كبار مســئولي المؤسســة. فبالتعاون مــع كبار الموظفــين في الإدارة ولجنة التدقيــق، يجب على الفريق الإداري المحدد أن يقوم بفحص أي مدونة موجودة للســلوك المهنــي ليحدد ما إذا كانت قواعدها وإرشــاداتها لا تزال صالحة لحوكمة الشركات في عصر قانون SOx. ســواء بالنســبة لعملية تنقيح المدونة الموجودة حالياً لقواعد السلوك المهني أو بالنســبة لتطوير مدونة جديدة، فإنه لا بد من تشــكيل فريق مكون من شريحة إدارية منتقــاة للقيام بهذه المهمة. بحيث يتعين على الفريق دراســة قضايــا الأعمال التي تواجه المؤسســة ومن ثم القيــام بصياغة مجموعة من قواعد المدونــة القابلة للتطبيق على هذه المؤسسة اعتماداً على أعمالهم والقضايا ذات الصلة. ويجب أن تكون قواعد المدونة مكتوبة بطريقــة واضحــة بحيث يمكن فهم مثل هذه النقاط بســهولة من قبل الجميع. الشــكل التوضيحي (٢٠-٢) يعرض أحد الأمثلة على موضوعات مدونة قواعد السلوك المهني. وعلى الرغم من أن هذه القائمة لا تنطبق على الجميع، فإن هذه الموضوعات تناسب العديد من المؤسسات الحديثة اليوم. فالنقطة الجوهرية هنا هي أن الرسائل المقدمة في المدونة يجب أن تكون واضحةً ولا لبس فيها. وقد شارك مؤلف هذا الكتاب بشكل كبير في صياغة مدونة قواعد السلوك لإحدى الشركات الأمريكية الكبرى منذ عدة سنوات.

شكل توضيحي (٢٠-٢)

مثال لموضوعات مدونة قواعد السلوك

فيما يلي الموضوعات الموجودة في مدونة قواعد سلوك نموذجية لإحدى المؤسسات

الأول: مقدمة:

أ. الغـرض من هذه المدونة لقواعد السـلوك المهني: بيان عام حـول خلفية هذه المدونة لقواعد السلوك.

ب. التزامنـا بالمعايـير الأخلاقية القوية: إعادة ذكـر بيان المهمة أو الرسـالة إلى جانب الخطاب المطبوع من الرئيس التنفيذي.

ج. أين تلتمس التوجيه أو الإرشاد: وصف لعملية الخط الساخن لأخلاقيات العمل في المؤسسة.

د. الإبلاغ عن عدم الامتثال: إرشادات للمبلغين -كيف تُبلغ.

هـ. مسؤوليتك عن الإقرار بالمدونة: وصف لعملية الإقرار بالمدونة.

الثاني: التعامل العادل:

أ. ممارسة البيع لدينا: إرشادات للتعامل مع العملاء.

ب. ممارسات الشراء لدينا: إرشادات وسياسات للتعامل مع البائعين.

الثالث: السلوك في مكان العمل

أ. معايير تكافؤ فرص العمل: بيان التزام قوي.

ب. مكان العمل والتحرش الجنسي: بيان التزام قوي بالقدر نفسه.

ج. تعاطي المواد المخدرة وإساءة استخدام العقاقير: بيان السياسة العامة في هذا المجال.

الرابع: تضارب المصالح:

أ. التوظيف الخارجي: فرض قيود على قبول طلبات التوظيف من المنافسين.

ب. الاسـتثمارات الشـخصية: القواعد المتعلقة باسـتخدام بيانات الشركة لاتخـاذ قرارات تخص الاستثمار الشخصي.

ج. الهدايا والفوائد الأخرى: القواعد المتعلقة بتلقي الرشاوى وتلقي هدايا في غير محلها.

د. الموظفون السابقون: قوانين تحظر منح امتيازات للموظفين السابقين في مجال الأعمال.

هـ. أفراد العائلة: قوانين حول إسناد أعمال لأفراد الأسرة، يخلق تضارباً في المصالح.

الخامس: ممتلكات وسجلات الشركة:

أ. أصول الشركة: بيان قوي حول مسؤولية الموظف عن حماية الأصول.

ب. موارد نظم الحاسب الآلي: التوسع في بيان أصول الشركة ليعكس جميع الجوانب المتعلقة بموارد نظم الحاسب الآلي.

ج. استخدام اسم الشركة: هناك قاعدة، أن اسم الشركة يجب أن يتم استخدامه في التعاملات التجارية أو تعاملات الأعمال العادية فقط.

د. سجلات الشركة: هناك قاعدة فيما يتعلق بمسؤولية الموظف عن سلامة السجلات.

هـ. المعلومات السرية: قواعد حول أهمية الحفاظ على جميع معلومات الشركة السرية وعدم الكشف عنها لأطراف خارجية.

و. خصوصية الموظف: بيان قوي حول أهمية الحفاظ على المعلومات الشخصية السرية للموظف وعدم الكشف عنها لأطراف خارجية وحتى للموظفين الآخرين.

ز. منافع الشركة: يجب على الموظفين ألا يأخذوا من منافع الشركة ما لا يحق لهم.

السادس: الامتثال للقانون:

أ. المعلومات الداخلية والتجارة الداخلية: هناك قاعدة قوية لحظر الأعمال التجارية داخل الشركة أو الاستفادة من المعلومات الداخلية.

ب. المشاركات والأنشطة السياسية: هناك بيان قوي حول قواعد النشاط السياسي.

ج. الرشوة والعمولات الخفية: هناك قاعدة صارمة بشأن قبول رشاوي أو عمولات غير مشروعة.

د. التعاملات التجارية الخارجية: القواعد المتعلقة بالتعامل مع وكلاء أجانب بما يتماشي مع قانون ممارسات الفساد الأجنبية.

هـ. السلامة في أماكن العمل: بيان حول سياسة الشركة لتتوافق مع قواعد(*) OSHA .

و. سلامة المنتج: بيان عن التزام الشركة بسلامة المنتجات.

ز. الحماية البيئية: هناك قاعدة فيما يتعلق بالتزام الشركة لتتوافق مع القوانين البيئية المعمول بها.

(*) تمثل كلمة OSHA الحروف الأولى من كلمة Occupational Safety & Health Administration وهي إدارة السلامة والصحة المهنية الأمريكية، وتعد المنظمة أو المؤسسة الأكبر على مستوى العالم فى مجال السلامة والصحة المهنية فهي تختص بوضع معايير الحفاظ على السلامة والصحة المهنية للعاملين فى جميع المجالات، وتهدف إلى ضمان بيئة عمل آمنة وصحية لكل العاملين كما تسهم بفاعلية فى الحفاظ على الموارد البشرية ومن ثم رفع مستوى الجودة فى المؤسسات. (المترجم).

والمثال التالي مقتطف من تلك المدونة لقواعد السلوك الخاصة بقسم أصول الشركة:

إننا جميعاً نتحمل مسؤولية رعاية جميع أصول الشركة متضمناً ذلك المخزون والنقدية والموارد والمرافق وخدمات الموظفين الآخرين وموارد نظم الحاسب الآلي. فإذا كنت ترى أو تشتبه في أن موظفاً آخر يسرق أو يشارك في أنشطة احتيالية أو غير ذلك مما لا يحمي أصول الشركة كما ينبغي، فربما عليك الإبلاغ عن هذه الأنشطة إلى مديرك أو إلى مكتب أخلاقيات العمل.

تعد هذه الكلمات مثالاً جيداً على نبرة وأسلوب المدونة الجيدة لقواعد السلوك. ويضع المسؤولية على من يتلقى المدونة ويحاول شرح القضايا بطريقة لا لبس فيها، ويقترح الاستجابات للأفعال المتوقعة.

بالإضافة إلى موضوعات وقواعد المدونة، فإن العديد من الشركات قد وجدت قيمة في إضافة مجموعة من الأسئلة والأجوبة لترافق النقاط الموجودة في المدونة، الأمر الذي يسمح لقارئ المدونة أن يفهم القضايا على نحو أفضل، وكذلك أنواع الأسئلة التي ربما كثير من الموظفين البسطاء قد يسألون عنها فيما يخص قاعدة المدونة. إن مفتاح الوصول لمجموعة واضحة من قواعد السلوك المهني هو أنها يجب أن تكون واضحة ومفهومة بالنسبة للجميع. وقد يُشكل ذلك تحدياً فعلياً للتعديل بالنسبة لفريق مدونة قواعد السلوك.

إننا لم نقم بإدراج عينة من مدونات قواعد السلوك في هذا الكتاب، وذلك نظراً لاختلاف مدونات قواعد السلوك المهني لدى كل مؤسسة تقريباً من حيث الأسلوب والشكل والحجم. فبعض الشركات تنشر وثائق مفصلة إلى حد ما، في حين أن البعض الآخر يحتوي على الأساسيات فقط. ومن المؤكد أن مدونات السلوك المهني بطبيعتها ليست أسراراً تجارية للشركة، وتسفر الدعوات الموجهة إلى مكتب الاستعلامات أو العلاقات العامة بالشركة عن القيام بتجميع نسخ من عينات مدونة قواعد السلوك المهني لديهم.

إن الشركات العالمية لديها مشكلة أخرى عند قيامها بوضع مدونة لقواعد السلوك. فعلى الرغم من أن الشركة قد يكون مقرها في الولايات المتحدة، فإن عملياتها التشغيلية الرئيسية قد تكون منتشرة في جميع أنحاء العالم في مكان وجود المديرين الرئيسيين والموظفين وأصحاب المصلحة الآخرين من الذين لا يستخدمون اللغة الإنجليزية لغة أساسية لهم. وعلى الرغم من أن التكاليف الإضافية تتمثل في الترجمة، فإنه لابد من التفكير في إنتاج

نسخ من مدونة قواعد السلوك على الأقل باللغات الرئيسية المستخدمة في عمليات الشركة. وإذا كان هنــاك العديد مــن المواقع ولكن بها أعداد قليلة من أصحــاب المصالح الناطقين بلغة أجنبية، فإنه ســيكون من المناســب وضع ملخص لمدونة قواعد السلوك الأساسية بكل لغــة من اللغات المحلية. ومع ذلــك، ينبغي أن تؤكد تلك الإصدارات المختصرة التوجيهات نفسها للاحتيال المالي الخاص بالبنية الموجهة نحو الخدمة (SOA) الواردة في مدونة قواعد السلوك الأساسية.

تبليغ أصحاب المصلحة بمدونة قواعد السلوك لضمان الامتثال بها:

يجب أن تكون مدونة قواعد السلوك للمؤسسة عبارة عن وثيقة حية. وستكون قيمتها قليلــة إذا ما تم وضعهــا وتوصيلها إلى جميع أصحاب المصلحة بكثــير من الضجة، ثم بعد ذلك تُحفظ في مكان بعيد وتُنسى. ســواء بالنسبة لمدونة جديدة لقواعد السلوك أو لمدونة موجودة تم تنقيحها بإضافة مزيد من التعديلات عليها، فإنه يجب على المؤسسة بذل المزيد من الجهد لتوصيل نسخة من هذه المدونة لجميع العاملين وأصحاب المصلحة. وتعد هذه خطوة أولى جيدة ســيكون من شأنها تقديم تلك النســخة الجديدة أو المنقحة من مدونة قواعد السلوك بشكل رسمي لكبار المســؤولين التنفيذيين في المؤسسة، وخصوصاً المسؤولين الماليــين. كانت مدونات القواعد الســلوكية في المــاضي تلقى أحياناً قبــولاً رمزياً فقط من مجموعة المسؤولين الكبار، مع شعورهم بأن تلك المدونات قد صُممت في الواقع للموظفين وليســت لهم. إلا أن الفضائح المالية التي تم الإبلاغ عنها والتي أدت إلى ســن قانون SOx في الســنوات الأولى من هذا القرن قد أبرزت في الواقع هذا التناقض. فكل من شركة إنرون Enron وشركة ورلد كوم WorldCom، (1) وهما الشركتان اللتان يتم الاستشــهاد بهما كثيراً كـ "أفراد الســوء" في عصر ما قبل سن قانون SOx، قد كانت لديهم مدونات كافية لقواعد الســلوك. ومع ذلك، فإن مســئولي الشركات لديهم بدوا كأنهم شــعروا بأن تلك القواعد لا يمكن أن تطبق عليهم.

ويمكــن اعتبار المدير المالي الســابق لشركة إنرون (Enron)، أندرو فاســتو (Andrew Fastow)، واحداً من الأمثلة المثيرة للقلق على عدم قبول كبار المســؤولين في الشركة لمدونة القواعد السلوكية. ولأنه كان على علم بأنه سيخالف مدونة قواعد السلوك بالشركة باتباعه

بعض المخططات المحاسـبية المشـكوك فيها غير المدرجة في الميزانية العمومية، فقد لجأ إلى لجنة التدقيق الخاصة بشركة إنرون وطلب منهم التصويت رسـمياً على إعفائه من مدونة قواعد السـلوك! وقد قامت اللجنـة بمنحه هذا الإعفاء، وكانت خطـوة أخرى على طريق الفشل الذي سارت فيه شركة أنرون ووصلت إليه في نهاية المطاف.

يجب على كبار مديري المؤسسة أن يُقروا رسمياً بأنهم قاموا بقراءة وفهم مدونة قواعد السـلوك وبأنهم سيلتزمون بها. وبمسـاعدة الفريق الإداري الذي يقف خلف تلك المدونة، فإنه ينبغي على المؤسسة أن تقوم لاحقاً بتعميم مدونة قواعد السلوك وإيصالها إلى جميع أصحاب المصلحة في المؤسسـة. وقد يتم ذلك على عـدة مراحل، وذلك عن طريق إيصالها أولاً إلى المرافق المحلية أو الرئيسـية، تليها الوحدات الأصغر، والمواقع الأجنبية، وغيرهم من أصحاب المصلحة. وبدلاً من أن تحتفظ المؤسسـة بنسخة من مدونة القواعد السلوكية مع مسـتندات المرتبات، فإنه يجب عليها بذل الجهود لكي تعرض تلك المدونة بطريقة تجذب الأنظار نحوها.

يمكـن إيصـال المدونة الجديـدة ونشرها من خلال وسـائل مثل المؤتمـرات الإلكترونية (Webinar) التي يقودها الرئيس التنفيذي أو الجلسات التدريبية أو وسائل أخرى لتوصيل أهميتهـا ومعناها. هـذا بالإضافة إلى أسـاليب الاتصالات الخاصة التي يمكن اسـتخدامها لإيصـال المدونة لجماعات أخرى كالباعة أو المقاولـين، ولكن ينبغي أن يكون هدف الشركة هو الحصول على اعتراف رسمي من كل أصحاب المصلحة بأنهم سوف يلتزمون بمدونة قواعد السـلوك الخاصة بالمؤسسـة. ويمكـن تحقيق هذا عن طريق أحد نظـم الإنترنت أو النظم الهاتفية حيث يُطلب من كل أصحاب المصلحة في المؤسسة الرد على هذه الأسئلة الثلاثة:

١- هل تلقيت وقرأت نسخة من مدونة قواعد السلوك؟ أجب بنعم أو لا.

٢- هـل فهمت مضمـون مدونة قواعد السـلوك؟ الإجابة بنعم إذا فهمـت هذه المدونة لقواعد السلوك أو الإجابة بلا إذا كان لديك أسئلة.

٣- هل توافق على الالتزام بالسياسات والمبادئ التوجيهية الموجودة في هذه المدونة لقواعد السـلوك؟ الإجابة نعم إذا كنت توافق على الالتزام بمـا جاء في المدونة، والإجابة بلا إذا كنت لا توافق.

إن الفكرة بأكملها هي أن يُطلب من كل فرد ســواء كان موظفاً أم صاحب مصلحة أن يُقر بقبول مدونة قواعد السلوك الخاصة بالمؤسسة. يجب أن تُسجل تلك الردود باستخدام إحدى أشكال قواعد البيانات الحاســوبية بحيث يُدرج فيها اسم الموظف وتاريخ مراجعته والقبول أو عدم القبول. يمكن التعامل مع أي قضية من القضايا الناشــئة عن السؤال الثاني من خلال برنامج المبلغين عن المخالفات الذي ســيتم وصفه لاحقاً. والفكرة هي أنه يتعين على الجميع - كل أصحاب المصلحة - أن يســهموا في مبدأ مدونة قواعد الســلوك والموافقة على شروطها. وإذا رفض أحد الأشــخاص قبول المدونة لأســباب محــددة، فإنه يتعين على المشرفين أو غيرهم مناقشــة هذه المســألة مع هذا الشــخص للوصول في نهاية المطاف إلى اتفــاق. إن الموقف النهائي هنا هو أن المؤسســة يجــب أن تتوقع أن كل الموظفين متفقون على قبول مدونة قواعد السلوك للمؤسسة والالتزام بها. إن اتباع مدونة قواعد السلوك ما هو إلا واحد من قوانين العمل، وأن الامتناع أو التخلف المســتمر عن الالتزام بهذه القواعد ينبغي أن يكون سبباً للإيقاف عن العمل وإنهائه.

إن الفكــرة بأكملها والتــي تكمن وراء شرط الحصول على الاعــتراف بهذه المدونة هي تجنب أي عذر مســتقبلاً من نوع "لم أكن أعرف أن ذلــك كان قاعدةً" وذلك عندما تُوَاجه بــأن هناك انتهاك للمدونة. إنها لفكرة جيــدة أن يتم تطبيق هذه العملية الخاصة بقبول المدونة بصفة ســنوية أو عــلى الأقل بعد أي تنقيح لوثيقة المدونــة. كما ينبغي الاحتفاظ بملفات توثيق هذه الإقرارات بالمدونة بطريقة آمنة.

انتهاكات المدونة والإجراءات التصحيحية:

تلخص المدونة الســلوكية مجموعة من القواعد للسلوكيات المتوقعة في المؤسسة، والتي تكون على شكل إرشادات وتوجيهات موجهة لجميع أصحاب المصلحة — المسؤولين الماليين وغيرهــم كالموظفين في جميع المســتويات والمقاولين والبائعــين. فبالإضافة إلى عملية نشر مدونة قواعد الســلوك الخاصة بالمؤسســة والحصول على قبول أصحاب المصلحة بالمدونة، فــإن هناك حاجة إلى وجود آلية للإبلاغ عن انتهاكات المدونــة للتحقيق والتعامل مع تلك الانتهاكات.

إن الهدف المنشــود هو أنه إذا كانت المؤسســة تُصدر مدونة قوية لقواعد السلوك إلى جانب رسالة الرئيس التنفيذي عن أهمية الممارسات الأخلاقية الحميدة، فإنه من المتوقع أن يقــوم جميع أصحاب المصلحة باتباع هذه القواعد. ومع ذلك، فإننا جميعاً نعلم أن البشر هم البشر، وســيكون هناك دائماً بعض الذين ينتهكــون القواعد أو يحومون حول انتهاكها. لذلك تحتاج المؤسســة إلى إنشــاء آلية تســمح لموظفي الشركة أو حتى من خارج الشركة (الغرباء) بالإبلاغ عن الانتهاكات المحتملة للمدونة بطريقة آمنة وسرية. يمكن التعامل مع الكثير من آليات الإبلاغ من خلال الخط الســاخن للأخلاقيات أو المبلغين عن المخالفات كما سيتم مناقشته في القسم التالي. هناك انتهاكات أخرى محتملة يجب معالجتها على مستوى مختلف. فلنفترض أن هناك أحد المشرفين الرجال يُلمِّح بأن تقديم خدمات غير شرعية من قِبل إحدى الموظفات سيكون وسيلة جيدة للتقدم في المؤسسة. فإن مدونة قواعد السلوك فيــما يخص حظر التحرش الجنسي لن تقوم بالضرورة بإيقاف هذا المشرف، كما أن الموظفة لن تســتطيع في كثير مــن الأحيان إبلاغ المدير المباشر لهذا المشرف عــن هذا الانتهاك. لذا ينبغي وضع عملية لرفع بلاغات بجميع أنواع الانتهاكات الأخلاقية.

لا بــد من دعم مدونة قواعد الســلوك في المؤسســة بالإجراءات والــردود المخطط لها والموثقــة عن الانتهــاكات. فعندما يتم الإبلاغ أو العثور عــلى مخالفات أو انتهاكات كبيرة للمدونــة، فلا بد من إجراء التحقيقات، واتخاذ الإجراءات المناســبة، بغض النظر عن مرتبة ومكانة أصحاب المصلحة في المؤسســة المســؤولين عن تلك الانتهــاكات. فإذا كانت مدونة قواعد الســلوك تمنع عملية نســخ البرمجيات — وهو ما يجب أن يكون — فإن العقوبات الموقعــة على أحد العاملين في الطاقم التحليلي لإحــدى مكاتب المبيعات البعيدة يجب أن تكون هي العقوبات نفســها التي تقع على أحد كبار المســؤولين العاملين في مجلس إدارة الشركــة. في حــال كان الاثنان قد قرأا الحظر ووافقا عليه، فإنــه يجب أن تكون العقوبات الواقعــة عليهما متماثلة. خــلاف ذلك، قد يؤدي إلى خلق جو يبدو فيه أن هذه القواعد لا تطبق على الجميع بالوتيرة نفسها.

يمكن التعامل مع معظم الانتهاكات لمدونة قواعد ســلوك من خلال الإجراءات العادية للموارد البشرية في المؤسســة والتــي ربما تلجأ إلى عملية تقديــم النصيحة أو البقاء تحت

المراقبة بالنسبة للانتهاك الأول للمدونة، والتي قد تؤدي إلى إنهاء الخدمة في حال تكرارها. كما يجب إبلاغ السلطات الخارجية عن الانتهاكات التي تتعلق بأمور يبدو كأنها دعاوى مدنية أو جرائم محتملة، ليخرج الأمر بذلك عن سلطة المؤسسة. إن الهدف العام هو أنه يجب أن يكون لدى المؤسسة عملية معمول بها لتشجيع جميع أصحاب المصلحة على اتباع الممارسات الأخلاقية الحميدة، كما هو محدد في مدونة قواعد السلوك، كما يجب توفير آلية ملائمة للتبليغ عن الانتهاكات واتخاذ الإجراءات والتدابير النظامية المناسبة إذا تطلب الأمر.

الحفاظ على سريان المدونة:

يوجد العديد من القواعد الأساسية للسلوكيات الأخلاقية الجيدة وأيضاً للمؤسسة، لا تتغير من سنة إلى أخرى. فالقاعدة الموضحة في المثال في (الشكل التوضيحي ٢٠-٢) عن حماية أصول الشركة، التي تم الاستشهاد بها قبل قليل، قد نصت على أن جميع أصحاب المصلحة يتحملون مسؤولية العناية والاهتمام بأصول المؤسسة التابعين لها، سواء كانت ممتلكات أم نقدية أو موارد حاسوبية أو غيرها. وهذا النوع من القواعد الأخلاقية لا يتغير مع مرور الوقت، في حين قد يتعرض غيرها من القواعد إلى التغيير نتيجة ظروف العمل وعوامل أخرى. وقد قام مؤلف هذا الكتاب بتولي إدارة التدقيق الداخلي لإحدى الشركات الكبيرة للبيع بالتجزئة - سنطلق عليها اسم الشركة أ - التي كانت تمتلك في الأساس مدونة لقواعد السلوك تمنع الموظفين من العمل لدى الجهات المنافسة. وقد كان ذلك مناسباً عندما كان يعمل بائع في أحد مراكز التسوق لصالح الشركة (أ) بدوام كامل. وفي عصرنا الحالي الذي يتميز بأن هناك الكثير من العمل يكون بدوام جزئي، فإنه من غير المناسب أن أقول لبائع يعمل في أحد مراكز التسوق بدوام جزئي إنه أو إنها لن تتمكن من العمل بدوام جزئي لمتجر تجزئة آخر، ولنطلق عليها اسم الشركة (ب)، موجودة في مركز التسوق نفسه. لذا فقد تم هنا تغيير مدونة قواعد السلوك لتنص على أنه يجب أن يكون ولاء الموظف للشركة (أ) وليس للشركة (ب) فقط أثناء عمله في الشركة (أ).

يتعين على المؤسسات أن تقوم وبشكل دوري بمراجعة مدوناتها المنشورة للقواعد السلوكية، وأن يكون ذلك كل سنتين على الأقل للتأكد من أن الإرشادات لا تزال قابلة للتطبيق وسارية. إن التغييرات التي تتم على مدونة قواعد السلوك ينبغي ألا تعامل

باستخفاف. فإن أي تنقيح ينبغي أن يمر من خلال عملية الإعلان والتعميم نفسها التي تم استخدامها عند تقديم المدونات للمرة الأولى. ينبغي إيصال المدونة المنقحة لجميع أصحاب المصلحة إلى جانب شرح التغييرات مع المطالبة بقبول إعادة الإقرار، كما أسلفنا.

إن الموظفين الجدد وغيرهم من أصحاب المصلحة الملتحقين بالمؤسسة، يجب أن تُعرض عليهم مدونة قواعد السلوك الحالية، بالشرط نفسه وهو أن يقرؤوا ويقروا بما جاء بالوثيقة. ويمكن مشاهدة الفيديو المنشور على الإنترنت لشرح وتعليم الموظفين الجدد كل ما يتعلق بمدونة قواعد السلوك والتزام المؤسسة بها. وسواء تم تعديل المدونة أم لا، فإنه ينبغي أيضاً أن يُطلب من جميع أصحاب المصلحة، بصفة دورية، أن يُقِروا من جديد بأنهم قد قرؤوا وسيواصلون الالتزام بالمدونة.

إن التعديل الجديد لمدونة قواعد السلوك والمطالبة بإعادة إقرار أصحاب المصلحة يمكن أن تكون مهمة مكلفة وتتطلب موارد مخصصة من المؤسسة من إدارة الأخلاقيات والموارد البشرية والتدقيق الداخلي، وغيرها. وتمشياً مع بيان المهمة أو الرسالة، فإنه يجب على المؤسسة أن تُبْقِي مدونة قواعد السلوك والمبادئ الداعمة لها أمام جميع أصحاب المصلحة في جميع الأوقات. ويمكن تحقيق ذلك من خلال إشارات مستمرة لمدونة قواعد السلوك مثل ملصقات لوحة الإعلانات في جميع المرافق أو أسئلة وأجوبة توجيهية في مطبوعات أو عروض تقديمية في دورات تدريبية للموظفين.

المبلغون عن المخالفات وإدارات الخط الساخن:

تعد عملية الإبلاغ عن المخالفات من العناصر الهامة في حوكمة الشركات. والمُبَلِغ عن المخالفات هو الشخص الذي يخبر الرأي العام أو شخصاً ما في السلطة عن أنشطة مزعومة غير شريفة أو غير قانونية تحدث في إحدى الدوائر الحكومية أو مؤسسة خاصة أو عامة. قد يكون سوء السلوك المقصود هنا عبارة عن انتهاك لأحد القوانين أو القواعد أو اللوائح أو تهديداً مباشراً للمصلحة العامة، مثل الاحتيال أو الانتهاكات المتعلقة بالصحة والسلامة أو الفساد. قد يدلي المبلغون عن المخالفات بدعاويهم داخلياً لجهات التحقيق داخل المؤسسة، أو خارجياً لجهات رقابية أو جهات إنفاذ القانون أو لوسائل الإعلام أو المجموعات المعنية بهذه القضايا.

لقــد كانت برامج المبلغين عن المخالفات لعدة ســنوات تدور حول دعم قوانين التعاقد الاتحادية ولوائح الصحة والسلامة، وغيرها. كما هو مبين في الفصل الثاني من هذا الكتاب، فإن قانون SOx يقضي بأن تقوم لجان التدقيق للمؤسسة بوضع إجراءات من أجل "التعامل مع معلومات المبلغ عن المخالفات فيما يتعلق بمسائل المحاسبة أو التدقيق المشكوك فيها." وعندمــا تم تفعيــل قانون SOx للمرة الأولى، كان هناك الكثير من التكهنات بأن هذا البند الخاص بالمبلغ عن المخالفات في قانون SOx سيصبح بمثابة كابوس، متمثلاً في إقامة الدعاوى الجنائيــة على العديد من الشركات الأمريكية، من خلال تقدم العديد من الموظفين بطلبات للابلاغ عن المخالفات. إلا أن هذا الأمر لم يحدث حتى الآن، وحتى وقت نشر هذا الكتاب كان هنــاك عدد قليل من الشــكاوى المســجلة لمبلغين عن مخالفات فيــما يتعلق بقانون SOx قد تم رفعها، إلى جانب عدد أقل من إجراءات تســوية عادلة. وقد ثَبتَ أن العملية القانونية وسيلة صعبة لحل القضايا وتسويتها.

ومع ذلك، فإن المؤسسة بحاجة إلى معرفة دعاوى المبلغين عن المخالفات والتعامل معها باعتبارهــا عنصراً هاماً من عناصر حوكمة الشركات. كما يجب على المؤسســة إيجاد إدارة داخلية للدعم بحيث يمكن لأي أحد من أصحاب المصلحة أن يبلغ دون الإعلان عن هويته عــن أي مخاوف يشــتبه بها، كما يمكن أن يتوقع الإجراءات العلاجية المناســبة. وبناء على خبرتنا في إنشاء مثل هذه الإدارات لإحدى الشركات الأمريكية الكبرى، فإننا نطلق على هذا النوع من المرافق اسم الخط الساخن للأخلاقيات.

ينبغي أن تكون إدارة الخط الساخن للأخلاقيات في المؤسسة عبارة عن مرفق يعمل أربعاً وعشرين ســاعة في اليوم سبعة أيام في الأسبوع ٧/٢٤ بحيث يتمكن أي من موظفي الشركة وأصحــاب المصالح من الذين يلاحظون أي شــكل من أشــكال المخالفات مــن التبليغ عنها بشــكل سري ودون الخوف من عمليات انتقامية منه. وقد يتم رفع هذا الأمر إلى المنظمة أو إلى الســلطات التنظيميــة. يجب ألا يكون هناك أي عمليــات انتقامية ضد الموظف أو المبادرة باتخاذ إجراءات قانونية لاســتعادة التعويضات. حيث يمكن لهذه الدعاوى الخاصة بالمبلغ عن المخالفات إلحاق أضرار جسيمة بسمعة المؤسسة وكذلك على وظائف المديرين المتهمين. وفي الوقت الذي تطلب فيه قواعد قانون SOx من لجنة التدقيق أن تقوم بإنشاء

مرفق خاص للتبليغ عن المخالفات، فإن الإدارات الأخرى في المؤسسة كإدارة الموارد البشرية والتدقيــق الداخــلي وأخلاقيات العمل في الواقع تكون بحاجــة إلى إعادة الأمور إلى نصابها بشكل حقيقي.

يضــع برنامــج التبليغ عن المخالفات الذي أقــره قانون SOx تحدياً أمــام أعضاء لجنة التدقيــق. فالعضــو العادي للجنــة التدقيق التابــع لمجلس الإدارة قد يكــون مطلعاً على الاحتياجــات الخاصة للبرنامج الفعال للمبلغ عن المخالفات، ولكن من شــبه المؤكد أنه لن يكون مطلعاً على العمليات اللازمة لإنشــاء أحد هذه البرامج. ويمكن لمجموعات التدقيق الداخلي أو الموارد البشرية في معظم الأحيان أن تساعد لجنة التدقيق في وضع برنامج فعال للمبلــغ عن المخالفات الذي يتوافق مع متطلبات قانون SOx. إن البرامج الفعالة الخاصة بالإبــلاغ عن المخالفات تعــد واحدة من تلك المفاهيم التي قد يكون ســمع بها الكثير من المديرين التنفيذيين، ولكن استيعابهم لها قد لا يكون بالشكل الكافي. وتوفر الأقسام التالية مزيداً من المعلومات عن هذه البرامج.

القوانين الاتحادية الخاصة بالمبلغين عن المخالفات:

إن القوانــين الاتحاديــة الخاصة بالمبلغين عن المخالفات بــوزارة العمل الأمريكية U.S. Department of Labor (DOL) تديــر وتفــرض ما يزيد عن ٢٠٠ قانون من القوانين الاتحادية التي تغطي العديد من أنشــطة الأعمال لنحو ١٠ ملايين من أرباب العمــل و١٢٥ مليون عامل. تقتضي معظم قوانين العمل والســلامة العامة والعديد مــن القوانين البيئية حماية المبلغين عن المخالفات بالنســبة للموظفين الذين يبلغون عــن انتهاكات القانــون من قبل أرباب عملهم. وتُطبق قواعــد قانون SOx الخاصة بالمبلغــين عن المخالفات على جميع العاملين في المنظمات المســجلة في هيئة الأوراق المالية والبورصة الأمريكية، ويتعين على الشركات العامة أن تُوْلي اهتماماً خاصاً بحماية المبلغين عن المخالفات في الشركات التابعين لها. ويقتضي قانون SOx حماية المبلغين عن المخالفات من أصحاب المصلحة في الشركات المطروحة للتداول، مما لا يسمح لأي شركة عامة أو أي مسئول أو موظف أو مقاول أو وكيل في مثل هذه الشركات "أن يُقَال أو تُخفض مرتبته أو يُهَدد أو يتم إيقافه أو مضايقته، أو أي طريقة أخرى تنطوي على

تمييز ضد الموظــف في شروط وأحكام العمل نتيجة أي عمل قانوني قام به الموظف". تطبق تلك القوانين التشريعية عندما يقوم أحد الموظفين بتقديم معلومات أو يساعد في التحقيقــات التي تجريها الوكالة الفدرالية التنظيميــة أو وكالات إنفاذ القانون أو الكونجــرس أو موظفي الشركة عن أي ســلوك قد "يعتقد الموظف بشــكل معقول" أنه يشــكل انتهاكاً لقوانين ولوائح هيئــة الأوراق المالية والبورصة الأمريكية أو قوانين الاحتيال أو الملفات أو الإدلاء بالشــهادة أو المشــاركة فيها أو غير ذلك مما يساعد في الدعاوى - المعلقة أو على وشك أن تحفظ - التي تتعلق بأي انتهاك مزعوم. وبعبارة أخرى، فإن الموظف أو أصحاب المصلحة الذين يرصدون بعض المخالفات المالية وبعد ذلــك يقومون بالإبلاغ عنها، تتم حمايتهم قانونياً أثنــاء التحقيق في هذا الأمر والبت فيه.

في معظــم الحالات، نجد أن الأحكام الخاصة بالمبلغ عن المخالفات قد وضعت في المقام الأول لحمايــة الموظفــين الذين يظنون بأنهم قد اكتشــفوا بعض المخالفــات وليس لزيادة الضوابــط الداخلية للمنظمة. مــن الممكن أن تخضع جميع الإجــراءات المُتَخَذَة من قبل شــؤون الموظفين بحق الأشــخاص المبلغين عن المخالفات مثل تخفيــض المرتبة أو الإيقاف، لعقوبــات قانونية بموجب هذا القانون. وعــلى الرغم من عدم وجود العديد من التجارب المتعلقة بالمبلغ عن المخالفات المتعلقة بقانون SOx في الوقت الراهن، فإنه من المتوقع أن يقــوم كلٌّ من هيئة الأوراق المالية والبورصــة ووزارة العمل، وهما من الوكالات الفيدرالية على نطاق واســع، بحماية الموظفين المبلغين عن مخالفات المحاسبة والتدقيق. ويشير ذلك إلى أن الموظف أو صاحب المصلحة الذي يســجل شكوى للإبلاغ عن المخالفات سوف يكون محمياً حتى يتم حل هذه المسألة.

بموجــب قانون SOx، تعد جريمة أن يقوم شــخص "عن علم وبقصد الانتقام" بالتدخل في عمل أو كســب الرزق لأي شــخص - المبلغ عن المخالفات - يزود مســئول إنفاذ القانون بــأي معلومات صادقة تتعلق بارتكاب جريمة محتملــة لانتهاك قانون SOx. فأي موظف يبلغ عن مخالفة ويواجه بسبب ذلك ممارسات سلبية في العمل فإنه من المحتمل أن يصبح بمثابة "شاهد إثبات محمي".

يقتــضي قانون SOx أن تقوم لجان التدقيق بإنشــاء عملية لتلقي ومعالجة الشــكاوى الــواردة بخصوص المحاســبة وضوابطها الداخلية أو أي أمور تخــص عمليات التدقيق ومن أجل "رفع الموظفين لتلك الشــكاوي بشــكل سري وغير معلوم الهوية" فيما يتعلق بمسائل المحاســبة أو التدقيق المشكوك فيها. إن أصحاب المصلحة الذين يدركون أنهم لن يتعرضوا للفصل أو التمييز غير القانوني نظراً لعملهم بصفة مبلغين عن المخالفات، سيسعون إلى مد يد العون عن طريق تقديم الشكاوى إلى وزارة العمل أو البدء بإجراءات المحاكم الفيدرالية. أما الذي سيتضرر فإنه سيحتاج عادة إلى الحصول على المساعدة القانونية الآمنة للسعي إلى تقديم المســاعدة، وقد تتطلب هذه العملية المزيد من الوقت والتكلفة بالنســبة لكل من المبلغ عن المخالفات والشركة التي اتُهِمت بالمخالفة. فعلى ســبيل المثال، ولضمان التغلب عــلى الشــكوى المقدمة، يجب على الموظف قبــل الذهاب إلى وزارة العمــل أن يثبت بأن المبررات التميزية كانت عاملاً أسهم في حدوث هذا الإجراء الوظيفي الظالم في شأنه. ومع ذلك، فإنه يتم رفض موضوع الشكوى، إذا ما أثبت صاحب العمل "بالأدلة القاطعة" أنه كان سيتخذ الإجراء الوظيفي نفسه حتى في ظل غياب هذا النشاط المحمي.

ويحــق للموظف صاحب الحــق في مثل هذا الإجــراء المطالبة بالتعويضــات الكاملة، متضمنــاً ذلك إعادته إلى منصبه وإعــادة الأجر مع الفائدة والتعويض عن تكاليف التقاضي وأتعاب المحاماة. ومما يزيد الأمور تعقيداً، أنه يمكن للمبلغ عن المخالفات المتضرر أن يقوم باتخــاذ إجراءات على عدة جبهات، فقد يســعى لطلب الحماية بموجب القوانين الاتحادية (الفيدراليــة) وقوانــين الولاية، وكذلك بموجــب أي ميثاق تفاوض جماعي في هذا الشــأن. ويتعــرض أربــاب العمل لخطر مزدوج بســبب إجراءات المبلغ عــن المخالفات، من خلال المســؤولية التي تفرضها أحكام قانون SOx وكذلك القوانين الاتحادية وقوانين الولاية بشأن الفصل غير المشروع وأسباب مماثلة للإجراء. أضف إلى ذلك أنه، يمكن للمبلغ عن المخالفات المتضرر السعي للحصول على تعويضات تأديبية من خلال إجراءات قضائية منفصلة.

إذا حكمنــا من خلال الخبرات الإدارية والقضائية الســابقة في مجــال صناعات الطاقة النوويــة وشركات الطــيران، فإن قوانين حماية المبلغ عن المخالفــات يمكن أن تصبح حقول ألغــام للــشركات. فإذا كان الموظف يثير أي نوع من أنواع التأكيدات التي تثبت أعمالاً غير

قانونية في الأمور المحاسـبية والتدقيقية، فإن المبلغ عن المخالفات يكون محمياً تماماً حتى يتم التحقيق في المسـألة والحكم فيها. وسـيكون هناك العديد من المحامين المسـتعدين والحريصين على مساعدة المبلغ عن المخالفات ورفع الدعاوى، ولا سيما ضد الشركات الكبرى ذات الإمكانيـات المالية الكبيرة. وبالإضافة إلى ذلـك، فإن مجموعة كبيرة من وزارة العمل والمحاكم السابقين حاضرون في هذا المجال لدعم العقوبات التنظيمية والعلاجات الشخصية.

ومـن منظور خبرة امتـدت لأكثر من ٢٠ عاماً في مجال أنشـطة المبلـغ عن المخالفات التابعـة لقانـون SOx في الولايات المتحدة، ينبغي أن تسـعى المنظمـة المعنية إلى تحقيق تـوازن بين حقوق الموظفين في رفع مخـاوف مبلغي المخالفات والقـدرة على إدارة القوى العاملة. إن بيئة العمل الإيجابية تحتاج إلى أن يشـعر الموظفون بالحرية في رفع مخاوفهم إلى الإدارة وإلى آليات فعالة للتعامل مع أية مخاوف يتم إثارتها. إن البرامج القوية المتعلقة بالأخلاقيات التي تمت مناقشـتها في الأجزاء الأولى من هـذا الفصل تعد مهمة لإيجاد بيئة نأمل بأن تحد من النشاطات التي تستدعي الإبلاغ عن المخالفات.

قواعد الإبلاغ عن المخالفات وضوابط المؤسسة:

باسـتخدام قواعد قانـون SOx مثالاً على ذلـك يمكن لأي موظف أو أي شـخص آخر مـن أصحاب المصالح أن يصبح مـن المبلغين عن المخالفات، وذلك بالإبلاغ عن أي نشـاط غير قانوني أو غير لائق في مجال المحاسـبة والرقابـة الداخلية والتدقيق. وينبغي أن تكون هـذه العملية أكثر فاعلية عندما يكون المبلغ المحتمل عن المخالفات هو أحد أعضاء طاقم المحاسـبة للشركة الذي يسـمع عن خطط لبعض المعاملات الاحتيالية أو موظف يعمل في وحدة نائية لا يرتادها موظفو الشركة باسـتمرار، كوحـدة التدقيق الداخلي. فقد صُممت قواعد الإبلاغ عن المخالفات لتشـجيع أصحاب المصلحة للإبلاغ عن هذه الأفعال الاحتيالية أو غير المشروعة وتحمي إلى حد كبير الشخص الذي يبلغ عن تلك الأمور. وهذا يثير سلسلة من القضايا بشأن المدققين الداخليين ومراجعات التدقيق الداخلي خصوصاً.

إن الهدف من عملية التدقيق الداخلي التي تمت مناقشـتها في الفصل التاسع عشر من هذا الكتاب، هو مراجعة واكتشـاف مشـاكل الرقابة الداخلية وقضايـا التدقيق الداخلي. حيث يتم مراجعة نتائج التدقيق الداخلي مع الإدارة وتقدم في شـكل تقرير رسـمي حيث

يمكـن للإدارة وضع الخطوط العريضـة لخططها الرامية لاتخاذ إجـراءات تصحيحية. من ناحية أخرى، ماذا لو اكتشف فريق التدقيق الداخلي أن هناك مسألة من المسائل المتعلقة بالأمور المحاسبية أو الرقابة الداخلية أو التدقيق لم تُبَلغ بها الإدارة رسمياً في تقرير التدقيق؟ هل يستطيع أحد أعضاء فريق التدقيق الإبلاغ عن هذه المسألة بموجب الإجراءات الخاصة بالإبلاغ عن المخالفات؟ هل يمكن للمدقق الداخلي الذي يصادف مسـألة تخص المحاسـبة والرقابة الداخلية وأنها ليسـت جزءاً من عملية التدقيق المجدولة، أن يسـلك مسار حماية المبلغ عن المخالفات للإبلاغ عن تلك المسـألة؟ ماذا لو كان عضو من أعضاء فريق التدقيق الداخلي لا يـؤدي أداء جيداً ويخشى إنهاء الخدمة؟ وهل يمكن لهذا المدقق بوضعه المهتز أن ينبش في بعض النتائج المحتملة التي ربما تكون معتمدة على أوراق عمل سابقة، ويقدم تقريراً بها إلى جهة خارج إدارة التدقيق ليحصل على الحماية الخاصة بالمبلغ عن المخالفات والأمن الوظيفي حتى يتم تسوية المسألة؟

مـن الواضح أن فريق التدقيق الداخـلي يعد جزءاً مـن الإدارة، فالمدققون الداخليون يتحملـون المسـؤولية الأولى في الإبلاغ عن أي مسـائل غير نزيهة أو غـير قانونية تواجههم خـلال عمليـات التدقيق إلى إدارة التدقيـق الداخلي للبت فيهـا. لا ينبغي لأعضاء فريق التدقيق الداخلي أن يحاولوا العمل بشكل مستقل بصفة مبلغين عن المخالفات في جزء من عمل التدقيق الداخلي. بل يجب على التدقيق الداخلي أن يضع سياسـة واضحة تنص على أن أي أمور تخص المحاسـبة أو الرقابة الداخليـة أو التدقيق وتتم مواجهتها خلال مراجعة التدقيـق المجدولة، يجـب أن يتم توثيقها في أوراق العمل الخاصة بالتدقيق وإرسـالها إلى إدارة التدقيـق الداخلي للبـت فيها. يتعين على كل من فريـق التدقيق الداخلي وإدارات الأقسـام أو الوحـدات التي يتم تدقيقهـا؛ أن يفهموا أن الغرض مـن التدقيق الداخلي هو عدم السـماح لفريق مترصد من مبلغي المخالفات بتفقد دفاتر وسـجلات الإدارة. وأن يتم التحقيـق في أي بند من البنـود غير القانونية أو غير اللائقة والإبلاغ عنها من خلال العملية الطبيعية للتدقيق الداخلي.

قد تظهر حالة يكتشف فيها مدققٌ داخليٌ إسقاط إحدى المسائل المحاسبية أو المتعلقة بالرقابـة الداخلية من عملية التدقيق، وربما يحدث ذلك في عملية يقوم بها المدقق الأول

لمراجعة أوراق عمل. فالمدقق الداخلي هو أول من يتحمل مسـئولية الحصول على قرار في هذا الشـأن من إدارة التدقيق الداخلي حتى يصل الأمر إلى مدير التدقيق الداخلي أو لجنـة التدقيق. وفي حـال قيام المدقق الداخلي بتوثيق المسـألة والتبليغ عنها بينما ترى إدارة التدقيق إسـقاط أو تجاهل هذه المسـألة، فإن المدقق الداخلي وبكل تأكيد يكون له بعد ذلك الحق وعليه المسـئولية في أن يبلغ عن هذه المسـألة، وهو مفعم بالأمل، من خلال إدارة الخط الساخن للأخلاقيات الخاصة بالمؤسسة أو حتى من خلال هيئة الأوراق الماليـة والبورصـة. وينبغي أن تكـون إدارة التدقيق والعمليات الأخـرى المعمول بها في المكان المناسـب لمنع مثل هذه الحالة المُحْبِطـة للمدقق الداخلي الذي يقوم بالإبلاغ عن المخالفات.

إطلاق إدارة الخط الساخن للأخلاقيات في المؤسسة:

قامت العديد من المؤسسات اليوم بإنشاء إدارات الخط الساخن للأخلاقيات. ويحتوي معظمها على وسائل سرية لخط الهاتف تدار من خلال قسم الأخلاقيات أو الموارد البشرية أو مقدم خدمات مسـتقل. إن عمليات الهاتف المجاني هذه، التي تعمل عادة على أسـاس ٧/٢٤، تسمح لأي موظف أو صاحب مصلحة بالاتصال بشكل سري ودون ذكر الاسم وطرح سؤال أو الإبلاغ عن مصدر قلق، أو "يطلق الصافرة" على مسألة ما. تتمثل فكرة توفير مرفق مسـتقل في أن يتمكن جميع أصحاب المصلحة من طرح الأسـئلة أو الإبلاغ عن المخالفات المحتملة على أي مسـتوى. هذه الإدارات ليسـت مطلوبة من الناحيـة القانونية، ولكنها وسـائل تمكن الموظفين أو غيرهم من أصحاب المصلحة في أكبر المؤسسات من طرح الأسئلة أو الإبـلاغ عن تصرفات خاطئة محتملة أو طلب المشـورة. قد تكـون القضايا المبلغ عنها عبارة عن ادعاءات تتعلق بسرقة ممتلكات الشركة أو شكاوى من الموارد البشرية، أو لمجرد الاستفسـار عن القضايا المثيرة للقلق. في معظم الحالات، سيقوم عامل الهاتف بأخذ جميع المعلومات اللازمة، وطرح أسـئلة عند الحاجة، ومن ثم يقوم بتمرير الحادثة المبلغ بشـأنها إلى السلطة المختصة للتحقيق والبت فيها. ويقوم الموظف المختص في إدارة الخط الساخن عادة بتخصيص رقم محدد للمسـألة المبلغ عنها، ومن ثم فإن المتصل يسـتطيع أن يتحقق من الحكم في وقت لاحق.

تم تأســيس الخطوط الســاخنة للموظفين في العديد من المنظــمات الكبيرة بداية من منتصف التســعينيات من القــرن الماضي. يكون الموظفون المخضرمــون في الموارد البشرية في الغالــب هم المشــغلين المناســبين لتمتعهم بمهــارات خاصة للرد عل المســائل المتعلقة بالموارد البشرية، كالمعاملات والإجراءات الخاصة بأماكن العمل. أينما كانت أماكن ارتكاب المخالفات، فإنه يتم تحويل الحالة المسجلة إلى جهات أخرى كالإدارة القانونية مثلاً للتحقيق فيهــا. في بعض الأحيان نجد أن هذه الخطوط الســاخنة قد تحولــت إلى ما هو أكثر قليلاً من مجرد خطوط للتبليغ عن المخالفات، حيث استخدمت للتبليغ عن العديد من المشاكل والمخالفات الطفيفة إلا أنها كانت بشكل عام ناجحة جداً.

وعــلى الرغم مــن أنه تم تأســيس العديــد مــن إدارات الخط الســاخن للأخلاقيات والســلوكيات للرد على استفسارات الموظفين وتقديم بعض النصائح والإرشادات والتحقيق في الحوادث المبلغ عنها بشــكل إرضائي مناسب، فإنه باستخدام المبدأ نفسه نجد أن المرفق المنشأ بالفعل لبرنامج المبلغين عن المخالفات الخاص بقانون SOx يضع المزيد من الضوابط والمســؤوليات الجديــدة على عاتق هذه الإدارة. وعلى الرغم مــن أن العديد من جوانب المســاعدة الودية للخط الساخن للأخلاقيات يمكن أن تظل مطبقة، فإن القوانين الاتحادية للإبلاغ عن المخالفات تتطلب عمليات ذات طابع رســمي أكبر من ذلك بكثير، ولا سيما في مجالات مثل السرية والوثائق المطلوبة لكافة الســجلات، والمعالجة الفعالة لأي تحقيقات. وبالإضافة إلى ذلك، فإن الموظف الذي يتم اســتدعاؤه في ادعاءات تندرج تحت بند الإبلاغ عن المخالفات التابع لقانون SOx يكون محمياً قانونياً من أي اتهامات مضادة في المستقبل. في بعــض الحالات، نجد أنــه لا بد من حماية الموظف المبلغ عن المخالفات بحيث لا يمكن أن تكــون هنــاك أية إجراءات من أي نوع موجهة إليه مــن قبل صاحب العمل حتى يتم البــت في هذه المزاعــم أو الادعاءات. ومع ذلك، فمن أجل إنشــاء مرفــق خاص بالإبلاغ عن المخالفات في المؤسســة، لا بد من تعزيز الإجراءات الرقابية في جميع مرافق الخطوط الســاخنة للأخلاقيات والسلوكيات التي تم إنشاؤها لهذا الغرض. الشكل التوضيحي (٢٠-٣) يحتوي على مبادئ توجيهية لإعداد برنامج للخط الساخن للأخلاقيات يخدم أيضاً مرفق الإبلاغ عن المخالفات في الشركة.

شكل توضيحي (٢٠-٣)

المبادئ التوجيهية لإعداد مركز اتصال للإبلاغ عن المخالفات

- إنشاء خطوط هاتف مستقلة - يفضل أن تكون مجانية - بريد إلكتروني آمن للمرفق. يجب ألا تمر هذه الخطوط من خلال لوحات التوزيع الأخرى للشركة.
- تدريب جميع العاملين في المرفق على الأحكام الأساسية للقواعد الاتحادية الخاصة بالإبلاغ عن المخالفات. وكذلك وضع النصوص بحيث يسهل على المتصلين طرح نفس الأسئلة العامة.
- الإعلان عن المرفق والترويج له وتعزيزه في جميع أنحاء المؤسسة مع التأكيد على الإبلاغ عن كل الوقائع، وسوف يكون المتصل قادراً على التحقق من الحالة وسيتم التعامل مع جميع المتصلين دون السؤال عن هويتهم، كما لن يكون هناك اتهامات مضادة بسبب ما يقوم به المتصل.
- تنفيذ نموذج تسجيل لتسجيل جميع المكالمات. الاحتفاظ بتاريخ ووقت المكالمة، واسم المتصل أو هويته، وتفاصيل البلاغ.
- إنشاء عملية للتوجيه والتخلص بحيث يمكن تحديد حالة من لديه معلومات المكالمة وحالة أي تحقيق.
- إنشاء قاعدة بيانات آمنة لجميع بيانات المبلغ عن المخالفات مع حماية مناسبة من خلال كلمة مرور.
- العمل مع الموارد البشرية، ووضع إجراءات لحماية تامة من الاتهامات من أي نوع لأي مبلغ غير أن هذه الحماية تكون غير معلومة.
- وضع عملية لتصفية كل المكالمات التي تخص المبلغ عن المخالفات، وتوثيق جميع الإجراءات، إن وجدت.

إن وجود مرفق خاص للخط الساخن والتبليغ عن المخالفات الأخلاقية ستكون قيمته محدودة ما لم يتم إيصاله و"بيعه" لجميع أعضاء المؤسسة. وهناك طريقة جيدة لإطلاق هذه العمليات من البداية وهي عن طريق مدونة قواعد السلوك التي نوقشت سابقاً. حتى إن كان قد تم إطلاق هذا الخط الساخن بالفعل، يلزم إخطار الجميع بحقيقة أن هذا الخط يمكن أن يستخدمه أي شخص من مبلغي مخالفات محتملة تخص البنية الموجهة نحو الخدمة. ويجب أن يكون الهدف هو التحقيق في جميع المكالمات والحل الفوري لها - وخصوصاً المكالمات الخاصة بالإبلاغ عن المخالفات - داخلياً لتجنب المحققين والمحامين الخارجيين.

إطلاق برنامج أخلاقيات العمل وتحسين ممارسات الحوكمة المؤسسية:

إن برنامج الأخلاقيات القوي، المستند إلى بيان مهمة ومدونة قواعد سلوكية ذات معنى، يعد عنصراً أساسياً لأي برنامج شامل لحوكمة المؤسسة. إن الفضائح المحاسبية التي أدت إلى ظهور قانون SOx في السنوات الأولى من هذا القرن، كانت في أغلب الأحيان عبارة عن فضائح في المستويات العليا من المؤسسة، سواء كان ذلك بسبب تآمر أحد المسؤولين الماليين أو الرؤساء التنفيذيين الجشعين أم بسبب إحدى شركات المحاسبة التي لا تسمح بالاستفسار عن أي شيء. فقد قامت الفرق التنفيذية الموجودة في الشركات التي تعرضت لفضائح محاسبية بتأسيس قواعدها الخاصة مع إيلاء القليل من الاهتمام لباقي المؤسسة.

إن برنامج الأخلاقيات القوي سوف يحسن من ممارسات حوكمة الشركات للمؤسسة بأكملها وليس فقط من ممارسات الأشخاص الموجودين في المكاتب التنفيذية. ينبغي النظر في الإجراءات الخمسة التالية على أنها جزء من إطلاق إستراتيجية فعالة للأخلاقيات والإبلاغ عن المخالفات للمؤسسة بأكملها:

١- **سياسة الشركة:** يجب أن يتم إصدار بيان سياسة المؤسسة من قبل الإدارة العليا لضمان تشجيع جميع أصحاب المصلحة، بأنه تقع على عاتقهم مسؤولية لفت انتباه الإدارة حول المخاوف المتعلقة بالممارسات المحاسبية والمالية. يجب على بيان السياسة أيضاً أن يؤكد أن الإدارة لن تتسامح مع الانتقام من الموظفين الذين يبلغون عن المخالفات. يمكن للسياسة أن تساعد في تعزيز عملية "الباب المفتوح" لمعالجة القضايا، التي، في النهاية، هو النهج الأكثر فاعلية في الإدارة.

٢- **برنامج خاص بمخاوف وشكوك الموظفين:** يجب وضع برنامج لاستقبال ومعالجة جميع المخاوف والشكوك المقدمة من قبل الموظفين بشكل سري وعدم الكشف عن هوياتهم. وينبغي أن يتضمن البرنامج الفعال لمخاوف الموظف:

- منسقاً مركزياً لمعالجة الشكوك والمخاوف والتحقيق فيها.
- ضوابط لضمان إجراء التحقيقات الكافية باستمرار، مع التوثيق السليم الذي يصف القرار الصادر بشأن تلك الشكوك.

- آلية التغذية الراجعة لتقديم المشـورة للموظـف في التصرف وإبلاغه بالحكم المتعلق بالمسألة المبلغ عنها.
- عملية تقييم دوري لفاعلية البرنامج.

٣- **تدريـب المشرفين:** ينبغي إجـراء دورات تدريبية لجميع مشرفي الصف الأول والمديرين الآخرين حول كيفية الاستجابة بفاعلية للشكوك والمخاوف المطروحة من قبل الموظفين. تتصاعد المشاكل في كثير من الأحيان بسبب سوء الفهم بين الموظف ومشرفه أو مشرفته. فمـن الممكن أن تعود بعض حـالات العنصرية والتحيز والمحسـوبية إلى الطريقة التي يتعامل أو يعالج بها المشرف حالة معينة مع أحد الموظفين. ومن ثم هناك حاجة ماسة لتدريب فعال للمشرفين والمديرين على التفاصيل الدقيقة المرتبطة بالشـكوك والمخاوف المحتملة لدى المبلغين عن المخالفات.

٤- **إرشـادات للمقاولين:** نظراً لاحتمالية وقوع الشركات العامة في شباك الأعمال العنصرية أو التحيزية أو المحسوبية الناجمة عن المقاولين الرئيسين والمقاولين الفرعيين وغيرهم من الـوكلاء، لـذا ينبغي وضع آليات خاصة معمول بها، كتضمـين شروط محددة في العقود لحماية الموظف.

٥- **اسـتطلاع آراء الموظفين:** وينبغي أن تجري الشركات وبشـكل دوري مسـوحات للقوى العاملة لديها لتقييم الثقافة المؤسسية وقياس ما إذا كان لدى الموظفين الشعور بالحرية في إبداء مخاوفهم وشكوكهم.

سـواء أكانت شركـة كبيرة أم صغيرة، فجميعهـا الآن تخضع لقواعـد ومتطلبات قانون SOx. إن العمليات الخاصة بالأخلاقيات والإبلاغ عن المخالفات التي تمت مناقشتها في هذا الفصل تعتبر من الأمور الهامة لتحقيق التوافق مع قانون SOx والوصول كذلك إلى حوكمة مؤسسية رشيدة.

ملاحظة:

١. لمزيــد من المعلومــات حول شركة إنرون، وشركة ورلد كــوم والشركات الأخرى التي شــاركت في سن قانون ساربينز-أوكســلي يمكن العثور عليها في العديد من مصادر الإنترنت وكذلك كتاب روبرت مولر، Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, and ITIL (Hoboken, NJ: John Wiley & Sons, 2008).

الفصل الحادي والعشرون
تأثير حوسبة وسائل التواصل الاجتماعي

هناك العديد من الأنواع والأنماط الجديدة التي نمت في السنوات الأخيرة في تطبيقات ومفاهيم تقنية المعلومات، وقد رافق ذلك ظهور بعض التطبيقات الجديدة والهامة والقائمة على ما يعرف بنظم وسائل التواصل الاجتماعي Social Media Systems، التي جاءت بمسميات مثل فيسبوك وتويتر ولينكدإن وغيرها الكثير. فقد كانت هذه التطبيقات موجهة في البداية إلى المستخدمين المستقلين، لتتيح لهم إمكانية نشر الملاحظات والصور وغيرها من المواد المتعلقة برسائل الصداقة الشخصية على الإنترنت وبين الأصدقاء بشكل عام. وهناك العديد من الأمثلة على ذلك، كأن تقوم إحدى الطالبات بنشر صورتها وبعض تفاصيل الحفلة التي أقيمت في المدرسة الثانوية، أو أن يقوم آباء فرحون بنشر صور ومعلومات عن مولودهم الجديد. وتُعْرَف نظم وعمليات إرسال الرسائل هذه بصفة عامة بتطبيقات حوسبة وسائل التواصل الاجتماعي، فالعديد من رسائلهم تكون مختصرة جداً ويتم إرسالها عبر الرسائل النصية المتاحة على العديد من الهواتف الخلوية. تعد نظم التواصل الاجتماعي من الأدوات العظيمة، وقد فاقت شعبيتها شعبية البريد الإلكتروني المستخدم بكثرة في مجال الأعمال هذه الأيام، وذلك باعتراف وشهادة الجميع. ومن الطبيعي أن تتسبب تطبيقات حوسبة الشبكة الاجتماعية في كثير من الأحيان في إثارة بعض القضايا المتعلقة بحوكمة تقنية المعلومات عند استخدامها داخل بيئات عمل المؤسسات.

ليس الهدف من هذا الفصل تقديم إرشادات تفصيلية عن استخدام تلك النظم أو التطبيقات الخاصة بالحوسبة الاجتماعية أو عن جوانبها التقنية، لكن الهدف هو مناقشة قضايا حوكمة تقنية المعلومات عندما تتعرض المؤسسة التي تسمح بحرية استخدام تلك النظم أو حتى تثبيتها لقضايا متعلقة بحوكمة الحوسبة الاجتماعية والرقابة الداخلية. قد تكون هذه النظم جزءاً رسمياً أو غير رسمي من البنية التحتية لتقنية المعلومات في العديد إن لم يكن في كل المؤسسات اليوم، لذا يتعين على مديري المؤسسات أن يستفيدوا من بعض المزايا الإيجابية التي يمكن الحصول عليها من استخدام نظم وسائل التواصل الاجتماعي.

كـما يجـب عليهم أيضـاً أن يدركوا أن نظم وعمليـات تقنية المعلومات الخاصة بوسـائل التواصل الاجتماعي قد تشكل بعض المخاطر المرتبطة بحوكمة تقنية المعلومات للمؤسسات الموجودة في الوقت الحالي.

ما المقصود بحوسبة وسائل التواصل الاجتماعي؟

إن تطبيق أو نظام التواصل الاجتماعي عبارة عن موقع خدمة أو منصة أو موقع تقني على شـبكة الإنترنت يركز على بناء شـبكات أو علاقات بين مجموعات من الأشـخاص أو المستخدمين الذين يتشاركون الاهتمامات أو الأنشطة نفسها. قبل سنوات ليست بالبعيدة كان مفهوم تقنية المعلومات الخاص بنظام التواصل الاجتماعي غير معروف. إن مثل هذا النظـام للتواصل الاجتماعي لديـه العديد من الميزات والمخاطر في بعض الأحيان بشـكل أكبر من النظام التقليدي للبريد الإلكتروني الذي يتم من خلاله تعريف كل مسـتخدم على الشبكة من خلال عنوان البريد الإلكتروني الخاص به دون الحاجة إلى المزيد من المعلومات عن المشـترك. في حين على الجانب الآخر، يقوم الأشـخاص الذين يتشـاركون الاهتمامات والروابط بتسـجيل الدخول إلى أحد النظم الخاصة بالتواصل الاجتماعي، وذلك من خلال عمـل بطاقة دعوة أوتوماتيكية خاصة بهم، أو من خلال تقديم لمحة مختصرة عن سـيرة حياة المشترك. يحق لأعضاء الشبكة القيام بنشر صورهم أو معلومات عن سيرهم الذاتية، أو تعليقـات عن أنشـطتهم وأسرهم، أو في بعض الأحيان نشر آرائهم السياسـية أو غيرها مـن المواد. تعتبر جميع خدمات وسـائل التواصل الاجتماعـي تقريباً عبارة عن تطبيقات تعمل على شـبكة الويب، وتسمح للمستخدمين بالتفاعل عبر شبكة الإنترنت أو من خلال البريد الإلكتروني أو الوسـائل الخاصة بإرسال الرسـائل النصية الفورية. كما تسمح مواقع التواصل الاجتماعي للمسـتخدمين بتبادل الأفكار والأنشـطة والأحداث والاهتمامات من خلال شبكاتهم الشخصية.

في الحقيقـة، إن تطبيقات تقنية المعلومات الخاصة بوسـائل التواصل الاجتماعي كانت قد ظهرت وبشـكل جيد قبل عصرنا الحالي الذي يشهد حالياً انتشاراً واسعاً لشبكة الإنترنت وحتى قبل ظهور الحاسـبات الشخصية المحمولة. وفيما يلي بعض الاتجاهات الرئيسية في تطوير حوسبة وسائل التواصل الاجتماعي منذ بدايتها وحتى الآن:

• **١٩٧٨-١٩٨٩: تطبيقات من نوع واحد إلى قليل:** في الأيام الأولى لظهور أجهزة الحاسبات الشخصية (على سبيل المثال، Apple II أو IBM PC)، كان التطبيق الأول المتعارف عليه لوسائل التواصل الاجتماعي يسمى نظام لوحة الإعلانات أو نظام لوحة النشرة المحوسب Computerized Bulletin Board System (CBBS)، والذي أُنشئ في شهر فبراير من عام ١٩٧٨ بواسطة وارد كريستنسن Ward Christensen، الذي كان يعمل في شركة IBM[١]. وقد تم استخدام هذا النظام من قبل مجموعة من مطوري البرمجيات في شركة IBM ليقوموا بمشاركة الرسائل التي تتعلق بأوقات وأماكن الاجتماعات، وذلك لتقليص الوقت المهدر في المكالمات الهاتفية. وربما كان هذا التطبيق هو المثال الأول للتطبيقات التفاعلية التي يتجاوز فيها حد الرسائل المرسلة نمط الواحد لواحد ليصل إلى نمط واحد إلى قليل.

في الحقيقة فإن شبكة الإنترنت لم تكن شائعة في ذلك الوقت، إلا أنه سرعان ما انتشرت آلاف من نظم لوحات الإعلانات CBBS، بمسميات مثل فيدونت FidoNet في جميع أنحاء أمريكا الشمالية وغيرها من الأماكن، لتصبح أدوات مفيدة وذات شعبية متزايدة للاتصالات بين المستخدمين المتباعدين جغرافياً والذين كان بإمكانهم الوصول إلى هذه النظم من خلال أجهزة المودم الهاتفية.

• **١٩٩٠-١٩٩٤: نمو الإنترنت:** في أوائل تسعينيات القرن الماضي، كان استخدام الإنترنت متاحاً بداية فقط للمؤسسات الحكومية والعسكرية والأكاديمية. فقد توجب على مؤلف هذا الكتاب، أثناء قيامه بتأليف كتابه الأول عن تدقيق تقنية المعلومات، أن يبحث عن أحد معارفه في إحدى الجامعات المحلية لمنحه إذناً كتابياً لإنشاء حساب إنترنت يسمح له بالوصول إلى بعض الوثائق الخاصة بتدقيق تقنية المعلومات. ولكن، سرعان ما ظهر العديد من تطبيقات الإنترنت التجارية القائمة على المستهلك بمسميات مثل بروديجي Prodigy وكومبيوسيرف CompuServe. وسرعان ما تحولت هذه الخدمات إلى مقدمي خدمات الإنترنت Internet service providers (ISP) كما كان يطلق عليها سابقاً في المدن الرئيسية في الولايات المتحدة.

وسرعان ما لاقى القبول الزائد للمســتهلكين على الإنترنت تأييداً كبيراً من شركة أمريكا أون لاين AOL، وهي الشركة التي قامت بتسويق الإنترنت بقوة عن طريق نشر الملايين من أقراص الاشــتراك الخاصة بها، حيث تمكن المشــاركون من الوصول إلى الإنترنت، وإرسال رسائل البريد الإلكتروني، وشراء البضائع، والمشــاركة في مفهوم جديد مــن منتديات الإنترنت. هذا بالإضافة إلى الفرصة التفاعلية للانضمام الى المنتديات على الإنترنت وبث رسائل البريد الإلكتروني، كانت هذه التطبيقات هي الخطوات الأولى في التطبيقات التدريجية لوسائل التواصل الاجتماعي.

• **١٩٩٥-١٩٩٩: طفــرة الدوت كوم:** لقد شــهد هذا العصر طفــرة كبيرة في تقنيات الويب وأدوات الإنترنت. وقد اعتمدت معظم تلك التطبيقات الجديدة على المنتجات الاستهلاكية الجديدة وعلى عمليات التسويق. ولم يحدث في هذه الفترة أي تطور أو نمو في تطبيقات وسائل التواصل الاجتماعي يتجاوز حدود مواقع لوحة الإعلانات الموجودة.

فقد كان الاستثناء الوحيد في هذا العصر هو ظهور تطبيق SixDegrees.com، وهو من أوائل مواقع الويب الخاصة بالشــبكات الاجتماعية، وقد اســتمر خلال الفترة ١٩٩٧-٢٠٠١، وقد تمت تســميته وفقاً للمفهوم "ســت درجات من الانفصال"[٢]. وقد سمح هذا التطبيق للمستخدمين بإدراج الأصدقاء وأفراد الأسرة، والمعارف، كما سمح أيضاً للمتصلين الخارجيين بالانضمام إلى الموقع. وتمكن المســتخدمون من إرســال رســائل ونشر الإعلانات والحوارات النقاشية للأشخاص الذين هم من الدرجة الأولى أو الثانية أو الثالثة بالنسبة لهم، كما تمكن المستخدمون من مشاهدة الروابط مع الأشخاص الآخرين الموجودين على الموقع. فقد كان هذا التطبيق واحداً من التطبيقات الأولى لمواقع الويب الخاصة بشبكة التواصل الاجتماعي بالنمط نفسه الذي نشاهده هذه الأيام.

• **٢٠٠٠-٢٠٠٤: نمو الاتجاه نحو وســائل التواصل الاجتماعي:** على الرغم من أن المخاوف المتعلقة بقدوم العام ٢٠٠٠ Y2K لم تشــكل أزمة بالحجم الذي كان متوقعاً، ومن انحسار الطفــرة التــي حدثت في الدوت كوم، فإن هنــاك العديد من تطبيقات وســائل التواصل الاجتماعي الجديدة قد أطلقت خلال هذه الفترة، منها ماي سبيس MySpace، وفيسبوك Facebook، وفريندستر Friendster، ولينكدإن LinkedIn وغيرها. وسوف نناقش بعضاً من هذه التطبيقات بمزيد من التفصيل في الأقسام التالية.

وقد تم استخدام العديد من هذه التطبيقات الجديدة على نطاق واسع من قبل أشخاص من داخل المنظمات المؤسسية ومن خارج التطبيقات الخاضعة لسلطة المؤسسة. وعلى الرغم من أنه كان هناك دائماً بعض الأصوات المرتفعة على نطاق ضيق، فإن تطبيقات وسائل التواصل الاجتماعي قد سمحت للناس بإنشاء المحتوى والمشاركة في التعليقات دون مشاركة المنظمة — وهو توجهٌ هدامٌ في غالب الأمر!

أثناء هذه الفترة تم إطلاق تطبيق آخر على منصة الإنترنت، وهو وورد WordPress، والذي سمح للأشخاص الذين ليس لديهم معرفة بالبرمجة ببناء وإطلاق مواقع المدونات الإلكترونية أو المذكرات الشخصية أو مواقع المحتوى. فباستخدام هذه الأداة، يمكن لأي شخص أن يقوم باستضافة مدونة إلكترونية على موقع المجال الذي يمتلكه أو تمتلكه ولها السيطرة الكاملة على تصميمه ومحتوياته بصورة أساسية. وقد كانت هذه خطوة كبيرة نحو الصحافة الشخصية.

- **٢٠٠٥-٢٠٠٩: استمرار نمو تطبيقات الشبكات الاجتماعية:** استمر نمو وتطوير تطبيقات وسائل التواصل الاجتماعي، وذلك من خلال ظهور تطبيقات مثل يوتيوب Youtube، وهو موقع ويب خاص بتبادل ملفات الفيديو، حيث يمكن لأي شخص أن يقوم بنشر أي محتوى للفيديو. وقد ازدادت شعبية استخدام الهواتف الذكية بشكل كبير وملحوظ، في هذه الفترة، وأصبحت رائجة على نطاق واسع، ويمكن للمستخدم أن يحمل عليها مجموعة متنوعة من التطبيقات. ربما كان التطبيق الجديد والأكثر أهمية في وسائل التواصل الاجتماعي خلال هذه الحقبة هو تويتر Twitter، وهو تطبيق يستخدم للرسائل أو التعليقات الإلكترونية القصيرة، حيث يستطيع المستخدم أن يقوم بنشر رسائل تعتمد على المحتوى القصير ومتابعة الآخرين من خلال دفعات قصيرة من المعلومات. وسوف نقدم تويتر بمزيد من التفصيل في قسم لاحق.
- **٢٠١٠ وما بعدها:** استمر نمو استخدامنا لتطبيقات الوسائل الاجتماعية في هذه الفترة، الأمر الذي تسبب في ظهور العديد من القضايا والمخاوف المتعلقة بحوكمة تقنية المعلومات في المؤسسات هذه الأيام. فعلى سبيل المثال، قد شهدت الأحداث العالمية خلال الأشهر الأولى من عام ٢٠١١ ما أطلق عليه شعبياً اسم الربيع العربي، حيث تم الإطاحة بالقادة

السياسـيين المسـتبدين في كل من تونس ومصر وليبيا. وقد بدأت الاحتجاجات المناهضة للحكومـة في كل دولة من تلـك الدول بعد إجراء العديد من الاتصـالات والحوارات عبر وسائل التواصل الاجتماعي بواسطة الفيسبوك وغيره من الوسائل الأخرى. فقد رأى الناس الأحـداث التي آثارت غضبهم وقاموا بنشر تعليقاتهم وصورهم للآخرين، من الذين قاموا بنقلها لأشـخاص آخرين. وكانت النتيجة هي تصاعد موجات من الاحتجاجات الشـعبية التي سرعان ما أطاحت بتلك الحكومات.

وعلى الرغم من أن اسـتخدام الناس لمثل هذه الوسـائل الخاصـة بالتواصل الاجتماعي "فيسـبوك" للإطاحة بالحكومات الاستبدادية يعد واحداً من الأمثلة الحقيقية على السلطة القويـة لتلك الوسـائل، فإنها لا تزال تحمـل بعض التحديات التي تتعرض لها المؤسسـات هـذه الأيام. فمن الممكن أن تشـكل أدوات وخدمات وسـائل التواصل الاجتماعي بعض التحديات بالنسـبة لحوكمة تقنية المعلومات في المؤسسـات هذه الأيام. فإن هذه النظم تعتبر جديدة بالنسـبة للعديد من المؤسسـات الحالية، ولا تسـتطيع تلك المؤسسات التي لا تزال تسـتخدم النظم والتطبيقات التقليدية لتقنيـة المعلومات أن تكون في المكانة التي تسمح لها بسـهولة بتبني نظم وسائل التواصل الاجتماعي المفتوحة والمرنة. هذا بالإضافة إلى أنه سـيكون الأشخاص العاملون في المؤسسـة في الغالب عبارة عن مستخدمين يقومون باسـتخدام تطبيقاتهم الخاصة بحوسبة وسـائل التواصل الاجتماعي بشكل شخصي. الأمر الذي من الممكن أن يثير بعض المشـاكل المتعلقة بحوكمة تقنية المعلومات في حال لم تقم المؤسسة بوضع القواعد والإجراءات المناسبة التي تغطي العمليات التشغيلية لتلك الوسائل.

أمثلة على وسائل التواصل الاجتماعي:

سـتتناول الأقسـام التالية ثلاثة من أشهر تطبيقات وسـائل التواصل الاجتماعي التي يختلـف بعضها عن بعض كلياً (فيسـبوك ولينكـدإن وتويتر)، كما أنها سـتتناول بعض القضايـا المميزة الخاصة بالحوكمة المحيطة بكل تطبيق مـن هذه التطبيقات. لقد بدأ اسـتخدام كل تطبيق من هذه التطبيقات بشـكل شـخصي، إلا أن الناس قاموا بنقله إلى أماكن العمل من خلال الاتصالات التي يجرونها على نظم الحواسيب المحمولة والهواتف الذكية الخاصة بهم.

فيسبوك Facebook:

فيسبوك هو أحد خدمات ومواقع الويب الخاصة بالتواصل الاجتماعي التي تم إطلاقها في شهر فبراير من عام ٢٠٠٤ من قبل مارك زوكربيرج Mark Zuckerberg وعدد من زملائه القاطنين معه في السكن الجامعي الخاص بجامعة هارفارد Harvard، وسيلة للتواصل وتبادل المعلومات بين زملائه من طلاب الجامعة. كان تطبيق الفيسبوك في البداية مقتصراً فقط على طلاب جامعة هارفارد، ولكن سرعان ما امتد ليصل إلى الكليات الأخرى في منطقة بوسطن، ثم وصل إلى جامعة آيفي ليج Ivy League، ثم جامعة ستانفورد Stanford. وقد أخذ فيسبوك تدريجياً في نيل دعم طلاب الجامعات الأخرى عن طريق السماع قبل أن ينتقل بعد ذلك ليصل إلى طلاب المدارس وغيرهم من المستخدمين. أصبح نظام فيسبوك هذه الأيام يحظى بشعبية كبيرة ويستخدم من قبل الكثير والكثير من الأشخاص في جميع أنحاء العالم. كما أنه حل محل البريد الإلكتروني كوسيلة للاتصال بين الأفراد بالنسبة للعديد من الأشخاص هذه الأيام.

أصبح عدد المستخدمين النشطين لنظام فيسبوك في أغسطس ٢٠١٢ يزيد عن ٩٥٠ مليون بعد أن كان يستخدم من قبل مستخدمين محدودين في السكن الجامعي عام ٢٠٠٤، وما زال عدد المستخدمين لهذا التطبيق في تزايد مستمر. وقد بدأت شركة فيسبوك العمل على أنها شركة خاصة إلا أنها أصبحت مؤخراً شركة عامة.

تكون البداية الأولى للأفراد المستخدمين لتطبيق فيسبوك ناتجة غالباً عن تحفيز من أحد الأشخاص، وهو عادة ما يكون صديقاً شخصياً، يقوم بإرسال رسالة بريد إلكتروني إليهم طالباً منهم أن يصبحوا أصدقاءه على فيسبوك. وبعد ذلك سيُطلب من المستخدم الجديد بأن يقوم بإنشاء ملف شخصي، وإضافة مستخدمين آخرين كأصدقاء ليتبادلوا الرسائل والإشعارات التلقائية التي تنطلق عند تحديث ملفاتهم الشخصية. كما يمكن للمستخدمين الانضمام إلى مجموعات المستخدمين ذوي الاهتمام المشترك التي تم ترتيبها وتنظيمها من قبل مكان العمل أو المدرسة أو الكلية، أو غير ذلك من المعالم.

الانضمام إلى فيسبوك:

وبالنسـبة لكثير من محترفي الأعمال الرفيعي المسـتوى، يعتبر فيسـبوك أكثر من مجرد تطبيق تقنية معلومات. فهو في غالب الأمر مفهومٌ ربما يكون كبار محترفي الأعمال قد قرؤوا عنـه، حتـى وإن لاحظنا في كثير من الأحيان عدم فهم المدير التنفيذي نفسـه لهذا النظام، والـذي يتجاوز عـادة حدود التعليقات والأنشـطة التي يقوم بتبادلها مـع أبنائه وغيرهم مـن البارعين في تقنية المعلومـات. وقد يكون هذا حقيقياً خصوصاً إذا كان لدى المرء أبناء يسـتخدمون ويفهمون نظام فيسبوك وهم في سـن الجامعات أو المدارس الثانوية. فهناك ٦٠٪ من ملايين المستخدمين لفيسبوك هم دون سن ٣٥.

في كثير من الأحيان يشـارك الشـخص في فيسـبوك للمرة الأولى من خلال تلقيه رسـالة بريـد إلكتروني من قبـل أحد شركاء الأعمال أو الأقـارب طالباً منه أي يصبـح "صديقاً" له على فيسـبوك. الشـكل التوضيحي (٢١-١) يوضح الخطوات اللازمة لتسـجيل الدخول إلى الفيسـبوك. الفكرة هي أن الشخص يقوم بتسـجيل الدخول بالاعتماد على الدعوة الأولية الموجهة إليه، ومن ثم يمكنه الاتصال بالآخرين الذين هم أيضاً مستخدمون لفيسبوك. يمكن للأصدقاء على فيسبوك الاتصال مع الآخرين بطريقة متتالية بصفة أصدقاء الأصدقاء، الذين يمكنهم الاتصال لإنشاء شبكة واسعة.

استخدام فيسبوك:

إن تطبيق فيسـبوك أكـثر بكثير من أن يكون مجـرد بديل عن اسـتخدام نظام البريد الإلكتروني، فهو يسـمح لك بأن تقوم ببناء ملف شخصي خاص بك، ونشر أو إرسال الرسائل لـكل شـخص من الأشـخاص الموجودين على قائمة الأصدقـاء الخاصة بـك، لتقوم بتقديم الشروحات للأنشـطة التي تمارسها، ولتتبادل الرسالة مع أصدقائك على الفيسبوك، والعديد من الأنشـطة الأخرى. فقد تتشـابه إلى حد ما هذه الرسائل سواء كانت نصية أم صوراً مع محتويات البريد الإلكتروني أو الرسـائل النصية القصيرة المرسـلة من خلال الهواتف الذكية. ومن المؤكد أن تلك الرسائل المرسلة في بيئة السكن الجامعي تكون عادة عبارة عن تعليقات وصـور تتعلق بإحدى الحفـلات أو الأحداث التي وقعت مؤخـراً. وتكون في العادة مجرد

ملاحظات يتم إرسالها دون الحاجة للرد. ويمكن لمستخدم فيسبوك أن يقوم بإرسال مذكرة محددة أو سؤال إلى أي شخص أو لجميع الأشخاص الموجودين على قائمة أصدقائه. ويمكن عندئذ أن ترسل أو تُوَجّه تلك الرسائل إلى غيرهم.

شكل توضيحي (٢١-١)

خطوات الانضمام لفيسبوك

الخطوة ١.	**قم بزيارة موقع فيسبوك (www.facebook.com).**
الخطوة ٢.	قم بإدخال اسمك بالكامل، عنوان بريد إلكتروني سليم، وتاريخ الميلاد. وبالإضافة إلى ذلك، ينبغي عليك إدخال أكبر قدر من المعلومات الشخصية وذلك عندما ترغب في نشرها على حسابك في فيسبوك في القسم "حول"About". وهذا قد يشمل عنوان العمل، والخلفية التعليمية، وأي مجال من المجالات العديدة الأخرى الخاصة بالاهتمامات الشخصية. يمكن للمرء أن يضع أيضاً صورة رقمية، أو صورة لأحد الزوجين والأسرة، وغيرها من المعلومات الشخصية في هذا المكان. يمكن لمستخدم جديد في فيسبوك أيضاً اختيار "لا شيء مما سبق" لتكون مجرد اسم مع قليل من المعلومات الشخصية.
الخطوة ٣.	اختر كلمة مرور خاصة بك. إدخال كلمة مرور يسهل تذكرها من ستة أحرف على الأقل.
الخطوة ٤.	أكمل اختيار التحقق من الصورة. حدد الكلمات أو الأرقام المعروضة واكتبهم.
الخطوة ٥.	اقرأ شروط الاستخدام وسياسة الخصوصية الخاصة بالفيسبوك. ضع علامة داخل المربع لتعبر عن موافقتك على شروط كل منهما.
الخطوة ٦.	انقر على زر "اشترك!" في أسفل الصفحة وانتظر إعادة توجيه إلى صفحة الشكر لكم.
الخطوة ٧.	راجع صندوق البريد الإلكتروني الخاص بك وانقر على صفحة التأكيد من فيسبوك. فإنها سوف ترسل لك رابط التأكيد للتسجيل الخاص بك.

تستطيع منشورات الفيسبوك أن تعرض وصفاً تفصيلياً عن الحياة الشخصية لأحد الأشخاص ونشاطاته، وذلك، اعتماداً على مستوى الخصوصية الذي تم تحديده. على سبيل المثال، بعد الدخول إلى فيسبوك، يستطيع الشخص أن يدخل إلى أحد الأسماء المعروفة

والذي ربما يكون مُسَــجلاً في فيســبوك - أو إلى اسم أي شخص آخر لنفس الغرض - والنظر إلى الملف الشــخصي الخاص بهذا الشخص، وإلى آخر المنشــورات المرسلة من الآخرين، كما يســتطيع الوصول إلى أصدقاء ذلك الشخص على الفيسبوك، وحتى الاطلاع على منشوراتهم أيضاً. وســنتحدث بشــكل أكبر عن المخاوف المتعلقة بخصوصية الأعمال في هذا المجال في قسم لاحق، ولكن إذا لم يقم مستخدم فيسبوك بتحديد النشاط الذي يقوم به على فيسبوك عــلى أنه نشــاط خاص، فإنه يمكن لأحدهم أن يصل في بعــض الأحيان إلى معلومات تفوق الحد الذي يريده ذلك المســتخدم. على ســبيل المثال، قد يرى الشخص بعض الرسائل من نوع "شكراً لدعوتي لل. . . " التي تم إرسالها إلى أحد الأشخاص، وأحياناً مع صورة، وكذلك القدرة على الذهاب إلى صفحة فيسبوك للمرسل. هذه الرسائل المرسلة تبقى لفترة طويلة، ما لم يتم اتخاذ خطوات مدروســة لحذف الســجلات. وعلى الرغم من روعة كل هذا الأمر بالنسبة لحياة الطالب الجامعي، فإن المنشورات والأنشطة المسجلة قد تكون مصدراً لبعض المخاوف المتعلقة بالخصوصية وحتى المخاوف الأمنية في بيئة الأعمال.

ومــن الممكن أيضــاً أن يكون تطبيق فيســبوك مفيداً في بيئات العمل إذا ما اســتخدم وســيلة لبناء وإدارة فرق القوة العاملة. فعلى ســبيل المثال، بالنســبة للمشاريع التنفيذية للنظم الكبيرة - على غرار الجهود الوارد وصفها في الفصل الســادس عشر من هذا الكتاب حــول إدارة المشــاريع والبرامــج - فإن مدير المــشروع يمكن أن يطلب مــن جميع أعضاء فريق المشروع أن يقوموا بإنشــاء أو تحديث ملفات التعريف الخاصة بهم على فيســبوك ليتم تثبيتهم بوصفهم أعضاء في فريق المشروع. عندها ســيكون من السهل القيام بجدولة وإرسال أحداث المشروع، كما يمكن للمدير المسئول التعرف على المعلومات الأساسية لأعضاء الفريق والدخول إلى ملفاتهم الشخصية بطريقة أكثر لطفاً، على عكس ما يحدث عند قيامه بالوصول إلى سجلات الموارد البشرية التقليدية.

إن حديثنا هنا يُبرز فقط القليل من ســمات فيســبوك الآخذة في التوســع. يمكن للمرء الاشــتراك لتحميل منشــورات من مواقع ويب محددة، ونشر الرسائل أو التواصل من خلال الهاتف الذكي واستقبال رسالة عيد الميلاد التي يمكن نشرها لجميع أصدقاء هذا الشخص على فيســبوك. بالنسبة للمؤسسة التجارية، يتســبب تطبيق الفيسبوك في إثارة بعض المخاطر.

على سبيل المثال، من الممكن أن يقوم أحد الموظفين بإرسال شكوى فى منشور على فيسبوك تتعلق بجودة بعض منتجات الشركة أو حتى كفاءة أحد المديرين. فالرسالة التي أرسلت إلى أحد الأصدقاء على فيسبوك على أنها رسالة شخصية يمكن أن يرسلها هذا الصديق إلى أصدقاء الأصدقاء مكونين بذلك شبكة اتصالات واسعة النطاق والتي يكون لها أحياناً مردود على المؤسسة وبعض القضايا الخاصة المتعلقة بها. كما سنتحدث في القسم التالي عن القضايا القانونية الخاصة بوسائل التواصل الاجتماعي، حيث يوجد العديد هنا من قضايا حوكمة تقنية المعلومات.

على الرغم من امتلاك تطبيق الفيسبوك أداة خاصة لبناء صفحات أعمال المؤسسة، والتي تعد إحدى الأدوات القوية لتسويق جميع جوانب العمليات التجارية للمؤسسة، وأن هناك تصاعداً مستمراً في استخدام الفيسبوك باعتبارها إحدى أدوات الاتصال في مجال الأعمال، فإنه يستخدم عادة في هذه الأيام لغايات الاتصالات الشخصية وليس للأعمال التجارية. فإنشاء صفحة أعمال على الفيسبوك تعد من الوسائل الجيدة للترويج، وذلك لأن صفحات الأعمال على فيسبوك يمكن مشاهدتها من قبل الملايين من مستخدمي فيسبوك. تعد صفحات فيسبوك تلك بمثابة منصة إعلانية فعالة تقدم أساليب مبتكرة للتسويق عبر الويب، الأمر الذي يسمح بالتفاعل بين أصحاب الأعمال والعملاء. في الحقيقة فإن هذه الصفحات تذهب إلى ما هو أبعد من قضايا حوكمة تقنية المعلومات المذكورة في هذا الفصل، كما أنها تمثل تطبيقاً مؤسسياً قوياً وفعالاً.

لينكدإن LinkedIn:

لينكدإن هو أحد تطبيقات وسائل التواصل الاجتماعي التي تحظى بشعبية كبيرة، ويقوم هذا التطبيق على الشبكات الاجتماعية أو المهنية المرتبطة بالأعمال التجارية، ويستخدم لإجراء اتصالات شبكية بين العديد من المجموعات المهنية، كأعضاء AICPA أو خريجي الجامعات. يعد موقع لينكدإن أيضاً بمثابة منصة اتصالات شعبية بالنسبة للعديد من الفئات المهنية، كمديري المشاريع والمهندسين المدنيين، والجيولوجيين، والمدققين، وغيرهم الكثير. وتعمل تلك المنصة في جميع أنحاء العالم وبعدة لغات. وقد كان هناك أكثر من ١٢٥ مليون مستخدم مسجلين في لينكدإن حتى وقت نشرنا لهذا الكتاب.

كانــت المــرة الأولى التي تَعَــرَّف فيها معظــم المهنيين على تطبيق لينكــدإن من خلال اســتقبال رســالة بريد إلكتروني من أحد المشــاركين المهنيين مصحوبة بدعوة للانضمام إلى إحدى المجموعات الموجودة في لينكدإن، أو للقيام بتأســيس اتصال لينكدإن لبعض المصالح أو الاهتمامات المهنية المشــتركة. إذا كان الشخص المدعو جديداً على تطبيق لينكدإن، فإنه يطلب منه التســجيل عن طريق إرســال بعض المعلومات الشــخصية، والتــي تتعلق غالباً بسيرته المهنية. الأمر الذي يأخد طابعاً أكثر رسمية مما هو عليه في تطبيق الفيسبوك، الذي من خلاله يطلب من الشــخص أن يصبح أحد أصدقاء فيسبوك لشخص ما دون الحاجة إلى إدخال أي معلومات أو تقديم طلب ما.

عند التسجيل في لينكدإن عضواً في إحدى المجموعات المهنية، فإنه يُطلب من المستخدم أن يقوم بتوفير معلومات عن ســيرته المهنية وأصحاب العمل الحاليين والســابقين، وكذلك تواريخ تلك الوظائف وغيرها من المعلومات المهنية الشخصية. كما يوجد هناك حيز لنشر ســيرة ذاتية كاملة وإعلانات وغيرها من المواد. ويضم النظام أيضاً عملية تســمح للمسجل الجديد أن يطلب جهات الاتصال الخاصة بأرباب العمل والمهنيين السابقين لتقديمها كمراجع.

يسمح تطبيق لينكدإن للمستخدمين المسجلين بالاحتفاظ بقائمة تفصيلية بجهات الاتصال مع الأشــخاص الذين لديه معهم مســتوى معين من العلاقة تســمى زملاء Connections. يمكن للمســتخدمين أن يقوموا بدعوة أي شخص (سواء كان مستخدماً للموقع أم لا) ليصبح زميلاً Connection ضمن مجموعة الزملاء، إلا أن المتلقي للدعوة يستطيع اختيار "لا أعرف" ليقوم برفض الدعوة الموجهة إليه. يمكن استخدام زملاء لينكدإن بإحدى الطرق التالية:

- يمكن بناء شــبكة اتصال مكونة من الزملاء المباشرين لشخص ما، ويوصف الزملاء الأوائل بزمــلاء الدرجة الثانية، وأيضــاً يوصف زملاء الدرجة الثانية بأنهم زمــلاء الدرجة الثالثة. يمكــن أن يســتخدم هذا للحصول على تعريف لشــخص ما يرغــب في معرفته من خلال الاتصال المتبادل.
- ويمكن بعد ذلك أن يســتخدم لينكدإن في العثور على وظائف، وأشخاص، وفرص الأعمال التي أوصى بها شخص ما في شبكة اتصال أحدهم.
- يمكن لأصحاب العمل إدراج الوظائف والبحث عن المرشحين المحتملين.

- يمكن للباحثين عن وظيفة مراجعة الملف الشخصي لمديري التوظيف واكتشاف أي من جهات الاتصال الموجودة يمكن التواصل معهم من خلالها.
- يمكن للمستخدمين نشر الصور الخاصة بهم وعرض صور غيرهم للمساعدة في تحديد الهوية.
- يمكن للمستخدمين متابعة مختلف الشركات والحصول على إشعارات حول المنتجات الجديدة أو غيرها من المعلومات.
- تتطلب آلية الوصول المستخدمة في بوابة تطبيق لينكدإن جهات اتصال لمجموعة من المهنيين المرتبطين بعلاقة سابقة، أو بإدخال إحدى جهات الاتصال الخاصة بهم بنية بناء الثقة بين مستخدمي الخدمة.

ضمن حدود المجالات المتنوعة للموضوعات المتخصصة الموجودة في تطبيق لينكدإن، فإن مواقع هذا التطبيق تعد منتديات نقاشية نشطة تغطي العديد من المجالات المتخصصة في لينكدإن. على سبيل المثال، يتضمن موقع لينكدإن الخاص بالجمعية الوطنية لأجهزة التحكم في الشركات[٣] سلسلة من النقاشات النشطة. ويجوز لعضو لينكدإن المشترك في هذه المجموعة أن يقوم بطرح سؤال مثل: "كيف يجب على مجلس الإدارة أن يدير مدققيه الداخليين بشكل أفضل؟" وقد يقوم الأعضاء الآخرون في هذه المجموعة بالرد على هذا السؤال، وقد تكون النتيجة نشوب نقاش ساخن يستمر بين جميع الأطراف.

ولعل الأمر الأكثر أهمية في سمات الاتصالات المهنية الخاصة بتطبيق لينكدإن، هو أنه يشمل سلسلة من التطبيقات المتخصصة التي تهدف للحصول على إرشادات وظيفية وتحليل سير الأعمال، وتعزيز مبيعات المنتجات، وتعزيز الوعي بالعلامة التجارية، والتعامل مع مبيعات التذاكر، والتواصل مع المستثمرين وما هو أكثر من ذلك بكثير. إن تطبيق استطلاعات الرأي الخاص بتطبيق لينكدإن يعد من الأمثلة الجيدة على ذلك. فهو يتيح لمستخدمي لينكدإن إمكانية العثور بسهولة على إجابات لأسئلة تخص أبحاث الأعمال والسوق. فهو يسمح للمؤسسة بأن تقوم بطرح بعض الأسئلة، التي سيقوم تطبيق لينكدإن بتوزيعها على زملائك وعلى الملايين من المهنيين المتواجدين على الموقع. ومن الممكن أيضاً أن يتم مشاركة نتائج الاستطلاعات مع مستخدمي فيسبوك أو تويتر على الحساب

الخاص بالمؤسسة، أو القيام بإضافتها إلى موقع الويب الخاص بالمؤسسة. وهو يعمل تماماً مثل أي خدمة استطلاع أخرى: يمكن لمستخدمي لينكدإن أن يقوموا بطرح سؤال، وإضافة حتى خمسة ردود أو إجابات محتملة، واختيار مدة التشغيل. وبمجرد أن يتم استلام الإجابات ضمن المدة الزمنية المحددة، فإن لينكدإن سيقوم بمشاركة الإجابات مع الشبكات الاجتماعية التي تم تأسيسها أو المواقع الإلكترونية للمؤسسة. نظراً لوجود هذا الرابط القوي في تطبيق لينكدإن، فإن ردود الاستطلاع يمكن تقسيمها للتصويت حسب العمر أو الجنس أو الأقدمية ، وهو ما يسمح للإدارة بتحليل أسئلة مثل " هل إجابة الشخص الذي عمره ٢٥ سنة تختلف عن إجابة الشخص الذي عمره ٤٥ سنة؟" أو " هل تختلف إجابات الرجال عن إجابات النساء؟ ".

إن لينكدإن أكثر من مجرد تطبيق خاص بالأعمال التجارية، كما أنه لا يمتلك البيئة المفتوحة نفسها والمعرضة للمخاطر المحتملة التي يمكن أن نجدها في فيسبوك، فالرسائل المرسلة لأصدقاء فيسبوك يمكن بسهولة تعميمها وإعادة تعميمها على الآخرين. ومع ذلك، ونظراً لأن تطبيق لينكدإن يعتبر وسيلة للاتصالات والنقاش المهني بين مختلف الفئات المهنية المتخصصة، فمن الممكن للبيانات السرية للمؤسسة أن تتسرب بسهولة من خلال مواقع النقاش الخاصة بتطبيق لينكدإن. أحد مهندسي تطوير المنتجات، على سبيل المثال، قد يقوم بالاشتراك في موقع لينكدإن الخاص بمهندسي تطوير المنتج في المؤسسة. كجزء من المناقشات الجارية على الإنترنت عبر تطبيق لينكدإن، قد يقوم مهندس التطوير بالرد بشكل غير سليم على مناقشة عبر الإنترنت عن طريق إعطاء بعض المعلومات السرية للمؤسسة حول نقطة فنية دون أن يدرك طبيعة البيانات الصادرة عنه. أضف إلى ذلك، أن السيرة الذاتية لهذا المهندس قد تكون مفتوحة لشركات التوظيف الخارجي، ويكون هناك استنزاف محتمل لموارد الشركة.

تويتر Twitter:

كانت المرة الأولى التي سمع فيها العديد في الولايات المتحدة الأمريكية عن تطبيق تويتر Twitter في عام ٢٠١١، وذلك عندما حاول عضو الكونجرس الأمريكي، أنتوني وينر Anthony Weiner إرسال صورة خليعة له على تويتر إلى مساعدته في الحملة الانتخابية، إلا أن الصورة

قد أُرســلت بالخطأ إلى قائمة التوزيع الموجودة في حســابه على تويــتر (أو ما يُطلق عليهم المتابعون followers بلغة تويتر)[٤]. وسرعان ما نشرت الصحافة أن عضو الكونجرس آنذاك كان يرســل العديد من الرسائل المشينة الأخرى على حســاب تويتر. أجبرت هذه الأحداث وينر على الاســتقالة، ومن المؤكد أن حماقته قد تســببت في جعل العديد يسمع عن القدرة الهائلة لتويتر.

تويتر هو خدمة مجانية تســمح لأي شخص أن يقول تقريباً أي شيء لأي شخص آخر ما دامت رســالته لم تتجاوز ١٤٠ حرفاً، فهو نظامٌ يخاطب مســتخدمه "ما الذي تقوم به الآن" ويتخلل ذلك تواصل اجتماعي على الإنترنت. واستناداً إلى شعاره الذي يمثله الطائر الأزرق، فإن تويتر يمكن مســتخدميه من إرســال وقراءة تلك المنشــورات التي تعتمد على النص أو الرسائل القصيرة، المعروفه بشكل غير رسمي باسم "تغريدات Tweets"، والتي تُرسل في كثير من الأحيان من خلال الهاتف المحمول، إما عن طريق الرسائل النصية أو التطبيقات التي تم إصدارها لبعض الهواتف الذكية. وبوجود كل هذه التطبيقات الخاصة بالرسائل، فإن تويتر يعد واحداً من المواقع العشر الأولى الأكثر زيارة في جميع أنحاء العالم. ويشــير الاســتطلاع الذي أجرته شركة كومبيت دوت كوم Compete.com في شــهر فبراير ٢٠٠٩، إلى أن تويتر يشــكل الشبكة الاجتماعية الثالثة الأكثر استخداماً، وذلك استناداً إلى إحصائياتهم التي تدل على وجود ســتة ملايين زائر جديد في الشــهر وخمسة وخمسين مليون زيارة تتم على تويتر شــهرياً. وللمساعدة في شرح المصطلحات والمفاهيم الخاصة بتويتر، فإن الشكل التوضيحي (٢-٢١) يسرد البعض منها. وقد يلاحظ العديد من كبار المديرين استخدام موظفيهم لهذه المصطلحات أثناء قيامهم بإرسال تغريداتهم للآخرين.

شكل توضيحي (٢١-٢)

المصطلحات والمفاهيم الخاصة بتطبيق تويتر

- **تغريدة Tweet:** عندما تنشر أو تكتب ١٤٠ حرفاً على تويتر وتنقر إرسـال فهي تعد تغريدة أو تويتينغ tweeting.
- **تسـجيل حسـاب Handle:** عبارة عن اسم المسـتخدم على تويتر في شكل ducttape@. اسم شخصي قصير مشابهة لـ URL.
- **متابعة Follow:** هذا هو الإجراء الخاص بإضافة شـخص ما إلى قائمة الأشخاص الذين تتابعهم، مما يجعل تغريداتهم تظهر على الصفحة الرئيسية الخاصة بك.
- **الردود Replies:** وهذا يحدث عندما يكتب شخص ما تغريدة مباشرة على حساب المستخدم - ducttape@ أي ثرثرة في منشور هادئ - وأيضاً في كثير من الأحيان يكون دعوة للتواصل مع متابع آخر.
- **إعادة التغريد Retweet:** يعد هذا أسـلوباً لإعادة نشر تغريدة شـخص آخر، وتبقى التغريدة الأصلية بجانب حسـاب المؤلف سـليمة دون تغيير، ولكنك في الأسـاس تُظهر تغريدة شـخص ما إلى الأتباع، والعديد يستخدم هذا لإضافة محتوى ومعرفة المواد من الأشخاص الذين يتبعونه.
- **الرسـالة المباشرة DM:** هذا المصطلح عبارة عن رسـالة يتم إرسالها مباشرة إلى مستخدم آخر. يجب أن يكون هذا الشـخص متابعاً لك لتتمكن من إرسـال رسالة مباشرة له أو لها. وهذه تعد أداة مفيدة جداً للرسائل الخاصة.
- **الوسـم (هاشتاج) Hashtag:** وهي طريقة يستخدمها الأشـخاص لتصنيف التغريدات على سبيل المثال قد يستخدم الآخرون العلامة نفسها، ومن ثم تكون وسيلة فعالة للناس لعرض تغريدات ذات الصلة.

على الرغم من القدرات الهائلة لتويتر على متابعة وحمل سـيل كبير من الرسـائل المتعلقة بمجموعة كبيرة من الأشـخاص والموضوعات، فإن مسـتخدم تويـتر وأحياناً الموظف قد يقضي الكثير من الوقت في قراءة وإرسال هذه التغريدات. على سبيل المثال، قامت شركة بير أناليتكس (Pear Analytics) المعنية باسـتطلاع أوضاع السـوق التي يقع مقرها في سان أنطونيو بولاية تكساس الأمريكية، بتحليل ٢٠٠٠ تغريدة (منشؤها الولايات المتحدة وباللغة الإنجليزية) على مدى أسبوعين في أغسطس ٢٠٠٩ وتم تصنيف الرسائل إلى الفئات الست التالية(٥):

١- ثرثرة عديمة الجدوى - ٤٠ في المئة

٢- محادثة - ٣٨ في المئة

٣- قيمة تمرير الرسائل - ٩ في المئة

٤- الترويج الذاتي - ٦ في المئة

٥- الرسائل غير المرغوب فيها - ٤ في المئة

٦- أخبار - ٤ في المئة

تشير هذه النتائج إلى أن تويتر يحتوي غالباً على الكثير من "الثرثرة العديمة الجدوى"، وهو البند الأول في القائمة أعلاه. ولعل الميزة هنا هي أن هذه الرسائل تسمح للمغردين عبر تويتر أن يعرفــوا الناس من حولهم فيم يفكرون وماذا يفعلون وبم يشــعرون؟ في جميع الأحوال، فإن العديد من هذه التغريدات يشبه إلى حد ما جلسات الحوار التي كانت تتم بين موظفي الشركة أثناء تجمعهم بالقرب من مبرد الماء(*) في الماضي. كان المدير المخضرم في ذلك الوقت يرفض أو يحد من مثل هذه النشــاطات الخاصة بالدردشــة حول مــبرد المياه. لذا لا بد من عمل محاولات مشابهة للحد من استخدام الموظفين لوسائل التواصل الاجتماعي أثناء العمل.

ســواء نظرنا إلى مثال عضو الكونجرس السابق الفاســد وينر Weiner، الذي سبق الحديث عنــه، أو إلى أي من الأمثلة الحالية العديدة الأخرى، فإن تويتر يعد أداة قوية يمكن أن تشــكل مخاطر على المؤسسة إذا ما تم استخدامها بشكل غير لائق. فكما تحدثنا للتو عن أهمية مدونة قواعد الســلوك المهني للمؤسســة في الفصل العشرين من هذا الكتاب، والحاجة إلى إقرار بأن جميع أصحاب المصلحة المعنيين بها قد قاموا بقراءة وفهم المدونة ووافقوا على الالتزام بها، فإنه يجب على المؤسسة أن تُطلق سياسة مماثلة لتطبيقات وسائل التواصل الاجتماعي مثل تويتر.

الشكل التوضيحي (٢١-٣) عبارة عن مثال لسياسة المؤسسة المتعلقة باستخدام الموظف لتويتر، وذلك باستخدام العينة الخاصة بنا للشركة العالمية لمنتجات الحاسب. ويمكن تنفيذ سياسات مماثلة لفيسبوك وغيرها من تطبيقات وسائط التواصل الاجتماعي، أو يمكن صياغة السياســة بطريقة تتضمن تطبيقات وسائل التواصل الاجتماعي في المؤسسة، ويتجلى جوهر ذلك في أن مثل هذه السياسات يجب أن تُطلق بطريقة تجعل من جميع الموظفين وأصحاب المصلحة الآخرين يكونون على فهم للمقاصد والمخاطر المحتملة من أي من هذه التطبيقات الخاصة بوسائل التواصل الاجتماعي.

(*) تعني الدردشة العارضة بين مجموعة من عمال الشركة الذين لا يكونون على اتصال مباشر أثناء العمل ويلتقون في استراحة قصيرة عند مبرد الماء للشرب ويمكن تسميتها في هذه الأيام بـ "دردشة التدخين". (المترجم).

شكل توضيحي (٢١-٣)

عينة لسياسة الاستخدام الخاصة بتويتر

الغرض: تصف هذه الوثيقة اســتخدام حســابات تويتر الشــخصية خلال يوم العمل للموظف. وهي لا تنطبق على حسابات تويتر الخاصة بالشركة.

نظرة عامة: تدرك الشركة أن الشبكات الاجتماعية وأدوات التواصل الاجتماعي الخاصة بالموظف تقدم قيمة ما للشركة. ونتيجة لذلك، فقد وضعنا سياســة تســمح بمساحة صغيرة من استخدام تويتر أثنــاء العمل طالما تم العمــل ببعض المبادئ التوجيهية. إذا اعُتبِرَت المبادئ التوجيهية الواردة في هذه السياسة غير مقبولة، فإنه من ثم يُعْتَبر استخدام الموظف لتويتر أثناء العمل أيضا غير مقبول.

تقــدم هذه الوثيقة مجموعتين من المبــادئ التوجيهية. المجموعــة الأولى هي التي تنطبق على كل اســتخدام لتويتر يخص الأنشــطة المتعلقة الشركة، سواء في أوقات العمل أم في الأوقات الشخصية. المجموعة الثانية هي التي تنطبق على أولئك الذين يرغبون في اســتخدام تويتر أثناء العمل واستخدام حساباتهم للمساعدة في الترويج للشركة.

المبادئ التوجيهية لاستخدم تويتر في الشركة العالمية لمنتجات الحاسب:

١. عــدم الإفصــاح عن المعلومات السرية أو الخاصة على حســاب تويتر الخاص بــك. الإفصاح عن المعلومات التنافسية أو الأسرار التجارية يكون سبباً كافياً لإنهاء الخدمة.

٢. تحمل مســؤولية ما تكتب. تذكر أن "إمكانية" أن تقول شيئاً ما لا تعني "إجبارك" على أن تقوله. الكلــمات المكتوبة تكون أكثر صعوبة في التفســير من التفاعل اللفظي. تذكر أن ما تقوله ســوف يكون بسجل دائم. كن حذراً. كن ذكياً.

٣. كن صادقاً واستخدم الإفصاح الكامل. إذا كنت تتحدث عن أحد منتجات الشركة أو منتج يملكه الطرف المنافس، فمن مصلحتك أن تفصح أنك تعمل لصالح الشركة.

٤. احترم حقوق التأليف والنشر. لا ترسل النص أو الصور أو الفيديو الذي تم إنشاؤه من قبل شخص آخر دون الإســناد الصحيح. إذا كان لديك أسئلة حول قانون حقوق التأليف و/ أو استخدام بعض وسائل الإعلام، اتصل بالقسم القانوني.

٥. تويتر ليست بديلاً للاتصالات داخل الشركة. فيجب أن تنتقل المعلومات الهامة من خلال قنوات الاتصال الطبيعية للشركة، وليس من خلال تويتر.

٦. تويــتر ليس بديــلاً لخدمة العملاء. رجاء قم بتوجيه العملاء إلى قســم خدمــة العملاء بدلاً من التعامل مع الاستفسارات بشكل كلي من خلال تويتر.

٧. كن واضحاً أنك لست الناطق الرسمي للشركة وأن وجهات نظرك لا تعكس بالضرورة وجهة نظر الشركة.

المبادئ التوجيهية لاستخدم تويتر في العمل: ١. الأمر يقتضي منك القيام بتقديم إما (أ) رابط لموقع الشركة أو (ب) شعار الشركة على صفحة تويتر الخاصة بك. ٢. أنت مطالب بأن تقوم بتنفيذ إحدى معاملات الشركة على حسابها الخاص على تويتر على الأقل مرة في الأسبوع. ٣. يجب أن يكون جزء من تغريداتك ذا صلة بالشركة و/ أو المجال الذي تعمل فيه. لا يوجد أي شرط يخص نسبة محددة يجب الوفاء بها من التغريدات، ولكن يعتبر ٢٠٪ من إجمالي التغريدات مستوى مثالياً. ٤. تذكر ضرورة أن تكون منتجاً، ذلك أن تويتر يمكن أن يبتلع وقتك ويمكن أن يمنعك من إكمال المهام الأخرى المتعلقة بالعمل. فاستخدم حكمتك لضمان أن يكون لديك متسع من الوقت لاستكمال جميع الأعمال العادية الخاصة بك.
لقد قرأت هذه السياسة الخاصة بالشركة العالمية لمنتجات الحاسب فيما يخص استخدامي لتويتر، وأنا أفهم إرشادات هذه السياسة، وأوافق على الالتزام بالقواعد والإرشادات الموضحة في هذه السياسة.

الاسم:------------------------------------.	رقم الموظف:---------------------------.
التوقيع:-----------------------------------.	التاريخ:---------------------------------.

نقاط ضعف حوسبة وسائل التواصل الاجتماعي في المؤسسة ومخاطرها:

من الممكن أن يكون التساؤل المنطقي الذي يدور بداخل أحد المسؤولين التنفيذيين هو، "أنا أحد كبار المديرين في المؤسسة. لماذا يجب عليّ أن أقلق جراء استخدام الموظفين وغيرهم من أصحاب المصالح لفيسبوك، وتويتر، وغيرها من أدوات التواصل الاجتماعي في بيئة العمل ماداموا ينجزون المهام الخاصة بهم؟ "هذا النوع من الأسئلة الذي يطرحه العديد من كبار المديرين عندما لا يدركون في الواقع طبيعة هذه التطبيقات التي تبدو في الظاهر أنها تطبيقات شخصية واجتماعية.

وكثيراً ما تبدو المواقع الخاصة بوسائل التواصل الاجتماعي أنها اجتماعية وخارج إطار الرقابة الخاص بمعظم نظم الأعمال وعملياتها واهتماماتها. وكثيراً ما ينظر إليها وكأنها فقط عبارة عن وسيلة تسلية للموظفين، مثل الجهود المشتركة التي تقوم بها لجنة التخطيط لإقامة حفلة الإجازة السنوية. ومع ذلك، فإنه يمكن للقضايا أو المسائل المتعلقة بوسائل

التواصل الاجتماعي أن تذهب إلى ما هو أبعد من مجرد أن تكون عبارة عن رسائل اجتماعية ودية، كاحتمالية أن يرى أشـخاص آخرون هذه الرسائل وأن يبادروا باتخاذ إجراءات معينة تستند إلى هذه الرسائل والمعلومات المتبادلة.

لقـد أبرزت المقالة الأخـيرة في صحيفة شـيكاغو تريبيـون Chicago Tribune كيف أن دردشـة الموظف على فيسـبوك يمكن أن تتسـبب في مشاكل للمؤسسـة. فقد تحدث الموظفون لدى تاجر سيارات باستخفاف فيما بينهم على الفيسبوك عن الطريقة التي يمكن أن يسـتخدمها صاحـب العمل لكي يتجاهل قوانين العمـل في الولايات المتحدة[٦]. وقد تم تمرير الرسائل التي كان من المفترض أن تكون خاصة بهم في نهاية المطاف إلى سلطات قانون العمـل في الولايـات المتحدة، الأمر الـذي أدى إلى اتخاذ الإجـراءات القانونية ضد صاحب العمل. إن الرسائل المرسلة من خلال نظم وسائل التواصل الاجتماعي تحمل بعض المخاطر!

يُنظر أحياناً إلى نظم التواصل الاجتماعي على أنها إحدى الموارد الخاصة بالموارد البشرية، وأنهـا إحدى النشرات غير الرسـمية للشركـة. ومع ذلك، فإن المؤسسـة تواجه العديد من المخاطـر المتعلقة بنظم وسـائل التواصل الاجتماعـي، والتي قد تتضمن فقدان السـمعة وخسارة المكانة المرموقة والتعرض للمساءلة القانونية، وذلك عندما يقوم الموظفون بإفشاء الأسرار ونـشر الصـور والفيديوهات المتعلقة بالأمور التي يجب أن لا يفعلوها. هناك أيضاً مخاطر أمنية على الحاسـبات الآلية من البرمجيات الخبيثة، وسرقة الهوية، وذلك من خلال ما يسمى التصيد الاحتيالي phishing، وخرق خصوصية البيانات الحساسة التي تم الحديث عنها في الفصل العاشر من هذا الكتاب.

إن المسؤولية عن المخاطر المرتبطة باسـتخدام الموظف لتطبيقات مثل فيسبوك وتويتر وغيرها من وسـائل التواصل الاجتماعي تتجاوز حدود إدارة أمـن تقنية المعلومات، حيث إن المسـؤولية الأساسية تقع على عاتق إدارة المؤسسة. حيث يتم تشغيل هذه التطبيقات بشكل عام عبر الإنترنت والنظم الخارجية الخاضعة لسيطرة الشركة.

ترتبـط العديـد من مخاطر تقنيـة المعلومات المتعلقة بوسـائل التواصـل الاجتماعي والمخاوف الإدارية بالسـلوك الفـردي الذي يحدث خارج حدود البنية التحتية للمؤسسـة ونظم تقنية المعلومات الخاصة بها. في جميع الحالات، فإن نظم وسائل التواصل الاجتماعي

تحمــل في طياتها قضايا تتعلق بالمحتوى وحرية التعبير. وترتبط هذه الممارســات الخاصة بوسائل التواصل الاجتماعي بشكل وثيق بالعديد من القضايا التي وردت في الفصل العشرين مــن هذا الكتاب الذي تحــدث عن الحاجة إلى وجود ثقافة أخلاقية في أماكن العمل. وهو الفصــل الذي تحدث أيضاً عن أهمية الرســائل والسياســات القوية لــلإدارة مثل مدونات قواعد الســلوك وبيانات المهمة أو الرسالة التي تساعد المؤسسة وأصحاب المصالح فيها على التفكــير بطريقة صحيحة وإيجابية. في جميع الأحوال، يجب على المؤسســة أن تكون على علم ببعض المخاطر والمخاوف المتعلقة بوسائل التواصل الاجتماعي التالية:

- **القضايــا المتعلقــة بإنتاجيــة الموظف:** ربما تميل هذه القضايا بشــكل أكــبر نحو الجانب الإداري من حيث تحديد أهداف الموظفين ومسئولياتهم، وإن كان الموظفون على مختلف مســتوياتهم يقومون أحياناً بقضاء وقت طويل في إرســال الملاحظات والصور لأصدقائهم، سواء كانوا من داخل الشركة أم خارجها، وسواء عبر تويتر أم عبر فيسبوك أو بعض تطبيقات وســائل التواصــل الاجتماعي الأخرى. ففــي بعض النواحي، قد لا يختلــف هذا كثيراً عن الأشخاص الذين يقضون أوقاتاً طويلة على المكالمات الهاتفية الشخصية، إلا أنه من الصعب القيام بمراقبة وكشف هذا النوع من الأنشطة الخاص بوسائل التواصل الاجتماعي.
- **نقص الرقابة المفروضة على المحتوى المؤســسي:** قد يقــوم الموظفون وأصحاب المصلحة بشــكل مقصود أو غير مقصود بنــشر معلومات خاطئة أو غير لائقة على مواقع وســائل التواصــل الاجتماعي. هذا النوع من المعلومات يمكن أن ينقل إلى العديد من الأشــخاص الآخريــن من خــلال الطبيعة التتابعية للعديــد من أدوات وســائل التواصل الاجتماعي. فبمجرد أن تبدأ المعلومات المغلوطة في النشر، فإنه يكون من الصعب إيقافها.
- **عدم الامتثال للوائح التنظيمية الخاصة بإدارة السجلات:** على الرغم من حقوق التأليف والنشر وقواعد حماية البيانات، فإنه من السهل جداً بالنسبة لأصحاب المصلحة أن يقوموا بنسخ وإرسال الوثائق المحمية عبر أنظمة وسائل التواصل الاجتماعي. وفي حال تم إرسال هذه السجلات بشكل غير صحيح أو غير قانوني فإن المؤسسة ستتعرض للمخاطر.
- **الفيروســات وبرامج التجســس:** يوجد هناك العديد من الحوادث المسجلة التي تم فيها اســتخدام وســائل التواصل الاجتماعي أو مواقع الشــبكات ذات الصلة لنشر البرمجيات

الخبيثة كالفيروسات[٧]، ومن المؤكد أن نظم التواصل الاجتماعي ليست الوسيلة الوحيدة المستخدمة في هذا الصدد. ومع ذلك، فإن مواقع الشبكات الاجتماعية على أرض الواقع ربما لا تشكل تهديداً أكثر من الذي يشكله أي نوع آخر من مواقع شبكة الإنترنت.

- **مشاكل عرض النطاق الترددي:** كانت مسألة عرض النطاق الترددي للبيانات Bandwidth تفوق بكثير أي مسألة أخرى في الأيام الأولى لظهور الاتصالات والإنترنت، فهو مصطلح يشير إلى "حجم القناة" أو كمية البيانات المنقولة عبر خطوط الاتصالات. إن إرسال الناس لكميات كبيرة من الصور الرقمية أو غيرها من المواد التي تعتبر إلى حد ما كبيرة الحجم قد تؤدي إلى اختناق النظام. وعلى الرغم من أن هذا الأمر لا يعد معضلة كبيرة بالنسبة لشبكة الإنترنت، فإنه يمكن لمثل هذا النوع من المواد الكبيرة الحجم أن تعيق خط الاتصالات لمؤسسة صغيرة ويؤدي إلى انسداده.
- **القضايا الأمنية للمؤسسة:** هناك العديد من الثغرات في هذا المجال. حيث يمكن أن يستخدم الجاني مثلاً الهاتف الخليوي للقيام بالتقاط صورة لإحدى الوثائق السرية أو المنتجات أو المرافق الموجودة، ويقوم بعد ذلك بكل سهولة ويسر بإرسال هذه المواد التي التقطها إلى شخص أو أكثر بواسطة أداة مثل فيسبوك من خلال بضع ضربات أو ضغطات سريعة على لوحة المفاتيح. ولذلك فإن هناك حاجة إلى ضوابط مادية وبيانات جيدة تخص سياسة التبليغ وبيئة أخلاقية قوية للمؤسسة.
- **قضايا المسؤولية في وسائل التواصل الاجتماعي:** يمكن أن تتحمل المؤسسة المسؤولية عن الرسائل التي تُرسل بواسطة أحد الموظفين خلال الوقت المخصص للعمل في المؤسسة، وذلك بالنسبة للمنشورات التي تتم بواسطة موارد تقنية المعلومات المؤسسية. وعلى الرغم من أن القانون حقيقة لا يزال غير واضح حتى الآن، فإنه وجد أن الأفراد هم المسئولون عن إرسال الرسائل التي تتطلب مزيداً من الحذر إلى مواقع الشبكات الاجتماعية. لذا يجب على المؤسسة ووحدات الأعمال توخي الحذر في مثل هذه الحالات، فهي بالتأكيد تشكل مخاطر يجب أخذها بالحسبان.

ولأن استخدامنا لأدوات التواصل الاجتماعي في ازدياد، فإنه لا يمكننا سوى أن نتوقع استمرار هذا التوجه أو التيار. ولأن معظم أصحاب المصلحة في المؤسسة لديهم أجهزة

هاتــف ذكي خاصــة، فضلاً عن اتصــالات الإنترنت الموجودة في منازلهــم، فإن جميع هؤلاء الأشــخاص تقريباً يســتطيعون الوصول إلى المواقــع الخاصة بوســائل التواصل الاجتماعي. البعــض من هؤلاء يقوم باســتخدام هذه الأدوات بشــكل مكثف، ومــن الممكن أن تصبح الحدود الفاصلة بين الأنشــطة الشخصية والنظم المكتبية ضبابية. وفي حال قامت المؤسسة بفرض سياســة منع استخدام وسائل التواصل الاجتماعي أثناء ســاعات العمل، فإنها بذلك تكون وكأنها تنظر إلى الموضوع عبر نظارة وردية. ونحن بشكل عام لا نعمل في المؤسسات فقط من الســاعة التاســعة صباحاً إلى الساعة الخامسة مســاء مثلاً، بل نحن منخرطون في الأنشــطة الخاصة بالأعمال أثناء وجودنا في المنزل وأثناء ســفرنا كذلك. ومن ثم لا يمكننا في مثل هذه الحالة أن نضع حدوداً فاصلة.

كما أن اســتخدام أدوات التواصل الاجتماعي في أنشطة الأعمال ينمو أيضاً. كما تحدثنا منــذ قليل عــن أداة الاقتراع الخاصة بتطبيــق لينكدإن، والتي يمكن اعتبارها نظاماً شــائع الاستخدام في أماكن العمل. وسنرى على نحو متزايد مدى تقارب وترابط الخطوط الفاصلة بين استخدام وسائل التواصل الاجتماعي في الأمور الشخصية أولاً وبين استخدامها في الأنشطة المتعلقة بالأعمال. إن السبيل الوحيد للحد من المخاطر والحصول على فهم أفضل لحوكمة تقنية المعلومات الخاصة باســتخدام أدوات التواصل الاجتماعي في أماكن العمل، هو إيجاد سياسات تتعلق بالاستخدام الفعال لهذه الأدوات وتبليغها بصورة جيدة إلى جميع أصحاب المصلحة في مكان العمل داخل المؤسسة.

سياسات وسائل التواصل الاجتماعي:

تحتاج المنشأة إلى وضع ممارسات تثقيفية توضح ما يجب الأخذ به وما يجب تركة من النظم المختلفة لوســائل التواصل الاجتماعي، هذا إلى جانب وضع سياسات محددة خاصة باســتخدام أصحاب المصالح لتلك الأدوات. ويجب أن تكون السياسات المتعلقة باستخدام وســائل التواصل الاجتماعي عبارة عن مجموعة فرعية من سياسات الشركة تماماً كمدونات قواعد الســلوك، وكذلك سياســات الأمن والخصوصية لتقنية المعلومــات التي يتم إيصالها لجميع الموظفين وأصحاب المصلحة. فلننظر على سبيل المثال إلى ما تم الحديث عنه بمزيد من التفصيل في الفصل العشرين من هذا الكتاب، حيث يتعين على المؤســســة وضع سياسة

محددة لوسـائل التواصل الاجتماعي لأصحاب المصلحة بشـكل عام والتي تحدد سياسات الشركة على مسـتوى عال جداً بأسـلوب يسـهل فهمه. كما يجب أن يتـم تنقيح المدونة وتحديثها بانتظام وينبغي أن يُطلب من جميع أصحاب المصلحة بأن يؤكدوا أنهم قد قاموا بقـراءة المدونـة وفهموها ووافقوا على الالتـزام بها. إن تنفيذ مثل هـذه المدونة لقواعد السـلوك يعد أمراً هاماً بالنسبة للممارسـات القوية والفعالة لحوكمة لتقنية المعلومات في المؤسسة. الشكل التوضيحي (٢١-٤) مثال على السياسة العامة لوسائل التواصل الاجتماعي في المؤسسـة والتي من شأنها أن تكون مصممة لتنطبق على جميع أصحاب المصلحة الذين يسـتخدمون تطبيقات وسـائل التواصل الاجتماعي في المؤسسة، بدءاً من الموظفين ووصولاً إلى الإدارة العليـا، ويمكـن تطبيق هذه السياسـة على جميع التطبيقات الخاصة بوسـائل التواصل الاجتماعي التي قد تؤثر في المؤسسة، سواء كان ذلك من خلال إحدى المبادرات أو التطبيقات المعتمدة على النظام والقائمة على المؤسسة أم من خلال استخدام أحد الأجهزة الشخصية.

شكل توضيحي (٢١-٤)

سياسة وسائل التواصل الاجتماعي في المؤسسة

تُطبق هذه السياسـة عـلى جميع أدوات التواصل الاجتماعي، وتسـتخدم داخل العمل وخارجه، بالنسبة لعمليات تشغيل الأعمال في المؤسسة. بالإضافة إلى الإرشادات الأكثر تحديداً التي تم مناقشتها أدناه، يجب على أي شـخص يسـتخدم أدوات وسـائل التواصل الاجتماعي في الأعمال الشـخصية أو التجارية ما يلي:

- تعامل مع الآخرين كما تحب أن تُعامل.
- أضف قيمة لعملائك، وصناعتك وعملك.
- اتسم بالاحترام والمهنية واللطف.
- قدم الرؤية، والخبرة، والدراسة ذات الصلة.
- تواصل أخلاقياً ومعنوياً في دعم أهدافك المهنية.

وبالإضافة إلى ذلك، يتعين على جميع أصحاب المصلحة في المؤسسة إبقاء المبادئ التالية في الاعتبار:

فكر قبل أن تنشر:

ضع في الاعتبار أن معظم منصات الحوســبة الاجتماعية على الإنترنت مثل الأسواق العامة، ما يتم عرضــه هناك يكون متاحــاً ويراه الجميع. على المنصات الاجتماعية، تكــون حدود المعلومات المهنية والشخصية دائماً غير واضحة. في هذه الأيام التي تتميز بتحويل سياسات الخصوصية والفهرسة القوية لمحرك البحث، لا يمكنك أن تكون دائماً على يقين مما يتم مشــاركته أو ما تم الاطلاع عليه أو ما تمت أرشفته. لاحظ أن ما تنشره على الإنترنت سوف يكون عام لفترة طويلة جداً. ما قمت بنشره سينعكس عليــك، لذلك التزم الطريقة التــي ترغب في أن تظهر بها أمام الشركة، والأصدقــاء، والعائلة، والزملاء، والعملاء. إذا كنت غير متأكد من أن محتوى معيناً مناســب لمشــاركته عبر الإنترنت، فلا تنشره. لأن تكون آمناً أفضل لك من الاعتذار.

المسؤولية:

أنت مسؤول شخصياً عن كلماتك وأفعالك، بغض النظر عن مكان وجودك، ما دمت موجوداً على شبكة الإنترنت. رجاء تذكر أنك عندما تشارك في وسائل التواصل الاجتماعي، فإنك تتحدث كفرد وليس نيابة عن الشركة. عرف نفسك دائماً باستخدام صيغة الإفراد لضمير المتكلم.

عندمــا تناقش معلومات تتعلق بالشركة على شــبكة الإنترنت، تحلَّ بالشــفافية من خلال إعطاء اســمك ودورك واذكــر أنك تعمل لصالح الشركــة. إذا كان لديك موقع فردي يشــير إلى الشركة أو له تأثير فيها، فاســتخدام إخلاء المســؤولية مثل "إن الآراء الواردة في هذا الموقع تخصني ولا تخص [اسم الشركة]."

أينما يســمح به القانون المعمول به فاعلم أن الشركة تحتفظ بالحق في مراقبة اســتخدام المنصات الاجتماعية واتخاذ الإجراءات المناسبة للحماية ضد إساءة الاستخدام التي يمكن أن تكون ضارة بسمعة الشركة.

أن تقوم بإنشاء حساب للشركة أو أن تصبح الممثل الرسمي الذي يتقاسم المعلومات حول الشركة ومجالات عملنا، يتطلب موافقة من المســتوى المناســب من الإدارة. هذه الحسابات فقط قد تعرض شعار الشركة.

السلوك:

يجب أن يكون سلوكك على الإنترنت متفقاً مع مدونة أخلاقيات العمل.

لديك فرصة للمسـاعدة على إظهار سـمعة الشركة على الإنترنت. استخدم خبرتك الواسعة لإثراء المناقشات، ساعد في حل المشاكل، وشاركنا الحماس في بيئة عملنا، وشجع التعلم ومشاركة الأفكار.

تذكر دائماً أن النغمة التي تسـتخدمها عبر الإنترنت يمكن أن تُفَسر بطرق مختلفة من قبل القراء، نظـراً لعـدم وجود تواصل شـفهي أو اختلافـات ثقافية. وقـد لا يكون بعض المشـاركين على دراية بالاختصارات والوجوه التعبيرية والرموز الشـائعة الأخرى المسـتخدمة في الاتصال عبر الإنترنت. تذكر أيضاً أن التعليقات تُنْتَزَع من سياقها غالباً، لذلك تمسك والتزم بالحقائق.

الثقـة هي العنصر الرئيسي في بناء علاقات عبر الإنترنت. بناء الثقة عن طريق الحفاظ على لهجة محترمـة، حتى عندما تختلف مع الآخرين، ومن خلال ردك على التعليقات في الوقت المناسـب أو في حينها. إذا كنت تدرك أنك قد أخطأت، حاول أن تصحح ذلك على الفور.

لا تشارك في أي سلوك على الإنترنت من شأنه ألا يكون مقبولاً في مكان عملك أو غير قانوني. على سـبيل المثال، لا تدلِ بتصريحات مهينة أو تستأسـد أو ترهب أو تضايق مستخدمين آخرين أو تسبهم أو تنشر محتوى يحض على الكراهية أو القذف أو التهديد، أو التمييز، أو الإباحية.

السرية:

قـم دائماً بحمايـة المعلومات السرية وغيرها مـن المعلومات المتعلقة بالملكيـة والخاصة بشركتنا وعملاءنـا ومورديـنـا. لا تضع أي محتوى على الإنترنت لا ترغب في مشـاركته مع صحفي أو عميل أو محلل أو منافس.

تأكد من أن أي إشـارة إلى معلومات تجارية وعملاء وموردين لا تنتهك أي التزامات عدم إفصاح. رجاء تذكر أيضاً التزامات السرية الخاصة بك بموجب اتفاقية العمل الخاص بك.

لا تفصح عن معلومات عن الزملاء أو غيرهم من الأشخاص، أو تسئ استخدام بياناتهم الشخصية، أو تنشر صورهم دون إذن منهم.

اسـتخدم دائماً الحكمة في التعامل مع المعلومات التي من الممكن أن تكون حساسة. لا تستخدم منصات الحوسبة الاجتماعية لتبادل المعلومات ذات الطابع السري للشركة أو العملاء أو الموردين، ما لم يتم إيقاف عملية الحصول على مثل هذا النوع من المعلومات وتم إزالة المحتوى من المنصة لمستويات أمنية مناسبة. المواقع العامة ليست المواقع المناسبة للاتصال الداخلي مع موظفي الشركة الآخرين.

حقوق الطبع والنشر: امتثــل للقوانين واللوائح، وعلى الأخص بالقوانين التي تحكم حقوق الملكية الفكرية، متضمناً ذلك حقــوق الطبــع والنشر والعلامات التجارية. يجب ألا تنشر محتوى أو تتخذ أي إجراء يخالف القانون أو ينتهك حقوق الشركة أو حقوق الملكية الفكرية لأي طرف ثالث.
أفكار أخيرة: استخدام منصات الحوسبة الاجتماعية وفقاً لهذه السياسة يمكن أن يكون أداة اتصال فعالة وقوية جداً. كونوا فخورين بما تعملون وتمتعوا بالشــعور بالإنجــاز في البحث عن أفضل جودة وكفاءة أكبر. قبل كل شيء، رجاء اســتخدم حكمتك وانتبه للآخرين وتحمل عناء الاســتماع وإيضاح فكرك بشــكل مفهموم.

اعتماداً على مستوى الاستخدام في المؤسسة، فإنه يمكن إطلاق سياسات مماثلة لفيسبوك، وغيرها من وســائل التواصــل الاجتماعي. وعلى الرغم من أنه يمكن صياغة سياســة عامة لكافة تطبيقات وسائل التواصل الاجتماعي للمؤسسة، فإنه يفضل عادة وضع بيانات سياسة محــددة لكل تطبيق، مثل تويتر وفيســبوك. والفكرة هي إيصال الرســالة لجميع أصحاب المصلحــة وهي أن اســتخدامهم لمختلف تطبيقات وســائل التواصــل الاجتماعي في أماكن العمل يحمل بعض المخاطر والفرص بالنسبة للمؤسسة ولمساراتهم الوظيفية.

إن تطبيقات وســائل التواصــل الاجتماعى تثير بعض القضايا القويــة الخاصة بحوكمة تقنيــة المعلومــات في المؤسســات هذه الأيام. وعــلى الرغم من أننا ركزنــا في هذا الفصل على تطبيقات فيســبوك وتويتر ولينكدإن التي ربما تكون الأكثر اســتخداماً هذه الأيام، فإن هــذا لا يضمن أن تبقى تلــك التطبيقات هي الأبرز خلال الســنوات القليلة القادمة. وفي جميع الأحوال، تمثل المفاهيم الخاصة بتلك التطبيقات تغيراً تاماً في طريقة تطوير ومعالجة البيانات والتي من شــبه المؤكد أنها لن تتغير. على الرغم من أن كبار المديرين قد ينظرون إلى هــذه التطبيقــات كما لو كانت عبارة عن أدوات لأطفالهم في المنزل أو في المدرســة، أو للموظفين الشباب في الكادر الوظيفي، فإنه يجب على كل واحد من كبار المديرين أن يصبح لديه ولو على الأقل مســتوى فهم بســيط بهذه الأدوات من أجل فهم أفضل لهم والتواصل مع الآخرين في المؤسسة.

ملاحظات:

1. Scott Gilbertson, "Feb. 16, 1978: Bulletin Board Goes Electronic," Wired, February 16, 2010, wired.com/thisdayintech/20100216/02/cbbs-first-bbs-bulletin-board/.

٢. يشــير مصطلح "ســت درجات من الانفصال" إلى فكرة أن كل شــخص على وجــه الأرض، من خلال طريقة التقديم، يبعد عن الآخر في المتوسط ست خطوات تقريبا، لذلك يمكن عمل سلسلة من بيانات "صديق الصديق" لتوصيل أي شخصين في ست خطوات أو أقل، في المتوسط.

٣. يمكــن للمدير التنفيذي الانضمام إلى موقع الجمعية الوطنية لمديري الشركات (NACD) عن طريق تسجيل الدخول إلى لينكدإن ثم النقر للانضمام إلى مجموعة (NACD). سيقوم مدير الموقع بمراجعة بيانات اعتماد الطالب وربما قبولها ومن ثم السماح لهم فيما بعد بالمشاركة في مناقشات الجمعية.

4. "Anthony Weiner Resigns: Timeline of Photos, Twitter Scandal Fallout," Huffington Post, June 16, 2011, www.huffi ngtonpost.com/201116/06//anthony-weiner-resignsscandal_n_878161.html; "Rep. Anthony Weiner Retains Lawyer amid Frenzy over Lewd Twitter Photo," Fox News, May 31, 2011, www.foxnews.com/politics/201131/05//rep-weiner-retains-lawyer-amid-frenzy-lewd-photo/.

5. Jennifer Van Grove, "Twitter Analysis: 40% of Tweets Are Pointless Babble," Mashable Social Media, August 12, 2009, http://mashable.com/200912/08//twitter-analysis/.

6. "Social Media Emerges as Battleground for Protected Speech at Work," Chicago Tribune, September 2, 2011, http://articles.chicagotribune.com/201102-09-/business/ct-biz-0902-chicago-law-20110902_1_social-media-labor-laws-employment-law.

٧. سوف يعرض البحث في جوجل العديد من الحوادث المبلغ عنها في هذا الصدد. وللاطلاع على إحدى عينات سجل الحوادث، انظر

"http://socialsmarty.com/small-business/should-social-networks-be-banned-at-the-workplace/."

الفصل الثاني والعشرون
حوكمة تقنية المعلومات ودور لجنة تدقيق تقنية المعلومات

تناولت الفصول السابقة العديد من الجوانب والعمليات اللازمة لفهم وتحسين حوكمة تقنيـــة المعلومات في المؤسســـة. وقد كان جميع ما تناولناه مــن تعليقات وتدابير مقترحة خاصة بحوكمة تقنية المعلومات موجهاً إلى جميع مؤسســـات الأعمال على اختلاف أنواعها وأحجامها، على الرغم من أننا ركزنا أكثر على الشركات الكبيرة المتعددة الجنسيات والوحدات والتــي تتجاوز غالباً الحدود الدولية. إلا أن بعض هذه الممارســات الخاصة بحوكمة تقنية المعلومات قد يكون أيضاً مكلفاً بالنسبة للمؤسسة الصغيرة، في حين أن البعض الآخر يتطلب مساهمات إدارية كبيرة. فعند تنفيذ أي عملية خاصة بحوكمة تقنية المعلومات، ينبغي على الإدارة دائماً النظر في التكاليف المترتبة على ذلك ومن ثم تُوازن بينها وبين المنافع العائدة.

ويختتم هذا الفصل الأخير بالحديث عن دور لجنة التدقيق التابعة لمجلس الإدارة، الذي يعد أحد العناصر الهامة جداً بالنســبة للشركة ولحوكمة تقنية المعلومات. إننا ننظر غالباً إلى لجنــة التدقيــق فقط من ناحية الدور الذي تلعبه في مهــام الإشراف والتدقيق الداخلي فضلاً عن قيامها بتنســيق أنشــطة التدقيــق الخارجي. حيث إن لجنــة التدقيق هي التي تقوم بتحديد نظام أو أســلوب العمل بالنسبة للعديد من الأنشطة الخاصة بحوكمة تقنية المعلومات. وسيقوم هذا الفصل بعرض الدور الذي تلعبه لجنة التدقيق من أجل وضع نظام أو أسلوب العمل المتبع لمراجعة الأنشطة الخاصة بحوكمة تقنية المعلومات في المؤسسة.

لجنة التدقيق التابعة للمؤسسة وحوكمة تقنية المعلومات:

تدار الشركات العامة من قبل مجالس الإدارة المنتخبين من قبل المســاهمين، والمسؤولة عن الأنشــطة الرئيســية للإدارة. ومن الممكن أن يكون أعضاء مجلس الإدارة المنتخبين في بعض الأحيان جزءاً من الكادر الإداري، أو أن يكونوا مديرين مســتقلين لا تربطهم بالشركة أية علاقات مباشرة. وتعد لجنة التدقيق أحد المكونات الرئيســية في مجلس إدارة الشركة، فهي المسؤولة عن مراقبة الضوابط الداخلية والتقارير المالية. ونظراً لهذه المسؤولية الرقابية

ومتطلبات قانون ساربينز أوكسلي (SOx)، فإنه يجب أن يكون أعضاء لجنة التدقيق مديرين مستقلين لا تربطهم أي علاقة بإدارة المؤسسة. لا يوجد أي قيود مفروضة على حجم اللجنة، إلا أن المجلس المكتمل المكون من ١٢ إلى ١٦ عضواً يمتلك غالباً لجنة تدقيق مكونة من ٥ إلى ٦ أعضاء. ومن الممكن أن تقوم لجنة التدقيق بدعوة أعضاء من الإدارة أو غيرهم لحضور اجتماعات اللجنة وحتى المشاركة في مداولاتها ونقاشاتها. ومع ذلك، لا يمكن للضيوف الخارجيين أن يكونوا أعضاء يتمتعون بحق التصويت بالكامل، وذلك بموجب قواعد قانون ساربينز أوكسلي SOx. إن مجلس إدارة المؤسسة هو الكيان الرسمي الذي يمنح مسؤولية الحوكمة الشاملة لمالكي ومستثمري ومقرضي المؤسسة. وقد يتحمل جميع أعضاء مجلس الإدارة المسؤولية القانونية عن أفعالهم التي يتخذونها حيال أي قضية، ويقوم المجلس ولجانه باعتماد معظم الأعمال الرسمية من خلال إصدار قرارات تصبح بدورها مواد ثابتة في سجل المؤسسة.

وكما هو واضح هنا، قد تكون مجالس إدارات الشركات مكونة مما يعرف بالمديرين الداخليين أو الخارجيين. فالمديرون الداخليون هم الأعضاء المنتظمون في الإدارة والذين يقومون أيضاً بالخدمة في مجلس الإدارة. مثل، الرؤساء التنفيذيين CEOs، والمديرين الماليين CFOs، والذين يلعبون أدواراً مزدوجة من خلال الإدارة التنفيذية لمهام العمل، ثم بعد ذلك الإشراف على العمليات التشغيلية للإدارة نفسها من خلال وجودهم في مجلس الإدارة. وباعتبارهم من كبار المديرين التنفيذيين في المؤسسة، فإنه يتعين عليهم امتلاك معرفة واسعة عن شركتهم، إلا أن تلك المعرفة لا تصب دائماً في مصلحة الخارج، وهم المساهمون والمستثمرون المستقلون. الأمر الذي أدى إلى ظهور انتقادات تصف المديرين الداخلين في بعض الأحيان بأنهم كالثعالب التي تحرس أقفاص الدجاج.

فالمدير الخارجي، أو ما يسمى غالباً بالمدير المستقل، هو الشخص الذي ليس لديه أي ارتباط مباشر بالعمليات التشغيلية اليومية للشركة، ولا يتقاضى أية رواتب أو أجور من الشركة جراء مشاركته في اجتماع مجلس الإدارة. يسافر المديرون المستقلون عادة إلى المدينة لحضور اجتماعات مجلس الإدارة، إذ إنهم لا يملكون مكاتب دائمة في المؤسسة وليسوا جزءاً من الكادر الوظيفي الخاص بها. حيث يُنظر إليهم على أنهم في وضع أفضل

لاتخـاذ القـرارات مثل إغلاق أحد المكاتـب، ولا ينظر إليهم على أنهـم يتصرفون لخدمة مصالحهم الشخصية.

في السـنوات التي سـبقت قانون سـاربينز أوكسـلي SOx، كان للعديد من الشركات مجالـس إدارة مكونة من مسـؤولي الشركة والأصدقاء والمقربين مـن المدير المالي CFO. وكانـت المجموعة الأخـيرة (المقربون) في بعض الأحيان غير مؤهلـة تماماً للعمل في هذه المناصـب في مجلـس الإدارة، وكانوا يتصرفون بموجب تعليـمات المدير المالي. وفي الواقع أصبح الوضع في غاية الصعوبة مع سـقوط شركة أنرون وإطلاق قانون سـاربينز أوكسلي SOx بين عامي ٢٠٠٢-٢٠٠٣. فقد اكتشـفت لجنـة الكونجرس الأمريكي التي حققت في كارثة شركة أنرون، من بين العديد من الأمور الأخرى، أن المجلس غير مسـتقل تماماً، وأنه قد اسـتفاد من "عقود الاستشارات" التي مُنحت له من قبل المدير المالي فضلاً عن وجود نقص واضح في الفهم الشـخصي للمعاملات الماليـة المعقدة الخاصة بشركة أنرون في ذاك الوقت.

لقد فرض القانون التشريعي سـاربنز أوكسـلي SOx، كما مر معنا في الفصل الثاني من هذا الكتاب، سلسـلة من المتطلبات الخاصة بمجلس الإدارة، والتي جاءت بهدف تحسـين حوكمـة الـشركات. كان من بين تلك المتطلبـات، أن لجنة التدقيـق الآن يجب أن تتكون فقـط مـن المديرين الخارجيين؛ الأمر الذي يمنحها اسـتقلالية تامة عـن إدارة الشركة، وأن تكـون، أو على الأقل ينبغي، أن تكون مؤلفة من مجموعة مؤهلة ومتخصصة من المديرين الخارجيين القادرين على فهم ومراقبة وتنسـيق وتقييم بيئة الضوابط الداخلية والأنشـطة الماليـة المتعلقة بالمجلس بأكمله. ولكي تتمكن لجنة التدقيق من الوفاء بمسـؤولياتها تجاه كل مـن مجلس الإدارة وأصحاب المصالح والجمهور، فإنها بحاجة إلى إنشـاء وإدارة وحدة خاصـة بالتدقيـق الداخلي والتي يجـب أن تكون عبارة عن مجموعة مسـتقلة من الآذان والعيون في المؤسسـة، وأن تقوم بتقديم التقييمات المتعلقة بالضوابط الداخلية وغيرها من الأمور الأخرى.

ويعتمد ذلك على بنية أو هيكل الشركة، كالشركات التي تتعامل بالأوراق المالية والمسـجلة لـدى هيئـة الأوراق المالية والبورصة الأمريكية، كما تسـتطيع الـشركات الخاصة الأخرى أيضاً

الاستفادة من هذه البنية الخاصة بلجنة التدقيق. على سبيل المثال، هناك العديد من المؤسسات غير الربحية أو الخاصة التي تكون كبيرة بما يكفي لتمتلك مجلس إدارة رسمياً ووحدة تدقيق داخلي رسمية خاصة بها. وعلى الرغم من عدم وجود نص صريح في كل من قواعد قانون ساربنز أوكسلي SOx وهيئة الأوراق المالية والبورصة الأمريكية يُلزم بذلك، فإن هذه المؤسسات ستستفيد أيضاً من لجنة التدقيق المكونة من مجموعة من المديرين المستقلين.

تتحمل لجنة التدقيق المسؤولية الكاملة عن مهام التدقيق الداخلي والخارجي للمؤسسة. فالمسؤولية الرئيسية للمدققين الخارجيين تجاه مجلس إدارة المؤسسة هي التصديق على دقة ونزاهة البيانات المالية. وعلى الرغم من استقلالية المدققين الخارجيين، فإن لجنة التدقيق تقوم بمراجعة الميزانيات الخاصة بالتدقيق الخارجي والتصديق عليها، كما تقوم باستلام التقارير الصادرة عنهم، وسيكون لها اتصالات مستمرة مع الشريك المسؤول عن عملية التدقيق. وعلى الرغم من أن مكاتب التدقيق الخارجي قد تقوم بخدمة إحدى المؤسسات على مدى عدة سنوات، فإنه يحق للجنة التدقيق القيام بتغيير المدققين الخارجيين في حال وجود خلافات حول الخدمات والميزانيات، أو غيرها من المسائل.

إن لجنة التدقيق هي المسؤولة عن التدقيق الداخلي وعن مدققي تقنية المعلومات لديها، والذين يلعبون دوراً كبيراً في عملية تقييم الضوابط الداخلية الموضوعة للتحقق من مدى موثوقية كل من التقارير المالية وعمليات تقنية المعلومات، وفاعلية وكفاءة العمليات التشغيلية، ومدى التزام المؤسسة بالقوانين واللوائح المعمول بها. ويقوم المدققون الداخليون وأخصائيو تدقيق تقنية المعلومات على وجه الخصوص بتقييم العديد من المخاطر المتعلقة بأمن وسلامة تقنية المعلومات وقضايا حوكمة تقنية المعلومات التي تواجه المؤسسة.

إن الإدارت الخاصة بالتدقيق الداخلي تكون محكومة من خلال الميثاق الذي تمت الموافقه عليه من قبل لجنة التدقيق، والذي يحدد أنشطتها وعلاقتها مع لجنة التدقيق في المؤسسة. وتتطلب تلك المواثيق عادة بأن تقوم لجنة التدقيق بالتالي:

- مراجعة الموارد والخطط والأنشطة، والتوظيف، والهيكل التنظيمي الخاص بوحدة التدقيق الداخلي في المؤسسة. وبالنسبة للأنشطة المتعلقة بحوكمة تقنية المعلومات، فقد تم إيجاز هذه المجالات في الفصل التاسع عشر من هذا الكتاب.

- مراجعة عمليات تعيين مدير التدقيق CAE وأدائه وتغييره، وهو الموظف المسؤول عن التدقيق الداخلي.
- مراجعة جميع عمليات التدقيق والتقارير المعدة من قبل وحدة التدقيق الداخلي بجانب مراجعة رد الإدارة.
- مراجعة مدى كفاية التقارير المالية ونظم الرقابة الداخلية مع كل من الإدارة ومدير التدقيق والمحاسبين المستقلين. ويتضمن ذلك نطاق ونتائج برنامج التدقيق الداخلي، والتعاون المتاح أو القيود (إن وجدت) التي كانت تفرضها الإدارة على سير عمليات برنامج التدقيق الداخلي.

ومع مرور الوقت شكلت هذه المتطلبات جزءاً من العلاقة التي تربط ما بين وحدة التدقيق الداخلي ولجنة التدقيق لديها. حيث يجب أن يعمل مدير التدقيق عن قرب مع لجان التدقيق للتأكد من مدى ملاءمة وكفاية الروابط الفعالة للاتصالات. والنقطة الثالثة المذكورة حول تقارير التدقيق تعد خير مثال على ذلك. فقبيل ظهور قواعد قانون ساربنز أوكسلي SOx، كانت بعض إدارات التدقيق الداخلي تقوم بتسليم لجان التدقيق التابعة لها فقط بعض الملخصات المتعلقة بنتائج تقارير التدقيق الداخلي، أو أنها كانت تقوم بتسليم نتائج تقارير التدقيق الداخلي التي يراها مدير التدقيق CAE بأنها "هامة". أما الآن فبموجب قواعد قانون ساربنز أوكسلي SOx، يجب على التدقيق الداخلي أن يزود لجنة التدقيق بجميع تقارير التدقيق وردود الإدارة الداعمة لها، ويتضمن ذلك أحياناً بعض التقارير التي تعتبر فنية إلى حد ما خاصة بتدقيق تقنية المعلومات التي تحتفظ بها إدارة التدقيق الداخلي، والتي جاءت من مراجعي لجنة التدقيق.

لا تشارك لجنة التدقيق عادة بالأعمال الإدارية اليومية الخاصة بإدارة التدقيق الداخلي ومديرها التنفيذي CAE، ولكنها يجب أن تضمن الجودة المستمرة لإدارة التدقيق الداخلي. فعلى سبيل المثال، يجب أن تقوم لجنة التدقيق بمراجعة خطط التدقيق السنوية بعناية، وأن تقوم بتوجيه الأسئلة المناسبة بشأن النتائج والتوصيات التي جاءت في تقارير التدقيق الداخلي. هذا بالإضافة إلى قدرة لجنة التدقيق على تعيين أو فصل مدير التدقيق CAE،

غير أنه يلزم وجود مستوى من التعاون المستمر في هذا الشأن. إذ لا تتواجد لجنة التدقيق في الموقع بشـكل يومي لتوفير الإشراف التفصيلي على عمليـة التدقيق الداخلي ويجب أن تعتمد على الإدارة العليا للمؤسسة من أجل الحصول على بعض الدعم التفصيلي.

لا يسـتطيع مديـر التدقيق أو المدققـون الداخليون تجاهل الطلبـات الإدارية الملائمة بدعوى أنهم مسـؤولون فقط عن توجيه تقاريرهم إلى لجنـة التدقيق، وبأنهم غير معنيين بالمسـار الإداري للمؤسسـة. وبالمثل، فإنه يجب على إدارة المؤسسة أن تكون واثقة من أن وحدة التدقيق الداخلي هي جزء من المؤسسة وليست وحدة خارجية أو غريبة عنها بسبب علاقتها مع لجنة التدقيق.

مسؤوليات لجنة التدقيق تجاه حوكمة تقنية المعلومات:

يجـب أن تقـوم لجنـة التدقيق بتطوير فهم شـامل لمجمـل احتياجـات التدقيق في المؤسسة. ويشتمل هذا التقييم العالي المستوى للاحتياجات على مختلف القضايا الخاصة بالرقابـة والتقارير المالية، الأمر الذي يسـمح للجنة التدقيـق بالقيام بتحديد الاحتياجات الخاصة بالتدقيق أو تقييم المخاطر، والتي سـتنفذ إما بواسطة وحدة التدقيق الداخلي أو بواسـطة مقدمي خدمات تدقيق آخرين. إن لجنة التدقيق باعتبارها جزءاً من هذا الدور وباعتبارها المنسـق النهائي لمجمل الجهود المبذولة في عملية التدقيق، هي المسـؤولة عن مراجعة واعتماد الخطط والميزانيات العالية المسـتوى الخاصـة بالتدقيق الداخلي. وعلى الرغم من أنه قد يكون لدى إدارة المؤسسة أفكارها الخاصة بأعمال التدقيق والكيفية التي يجب أن تُنفذ من خلالها تلك الأعمال، وعلى الرغم من المرئيات الخاصة للمدير التنفيذي للتدقيق CAE بخصوص الاحتياجات التي يجب أن تنفذ، فإن لجنة التدقيق هي المسؤولة عـن التصديق على الخطط والموازنات الخاصة بوحـدة التدقيق الداخلي. ولا بد من أخذ جميع المرئيات أو الآراء المختلفة للأطراف الرئيسـية بالاعتبار والعمل على تحقيق التوافق والانسـجام فيما بينها بشـكل مناسـب، إلا أن لجنة التدقيق هي صاحبة الكلمة الأخيرة والفاصلة في هذه المسائل.

وكـما وضحنا في الفصول السـابقة، كانت الإدارة العليا ولجنـة التدقيق التابعة لمجلس الإدارة تهتم عادة بقواعد المحاسـبة المالية، وقواعد قانون سـاربنز أوكسلي SOx، والقواعد

الشـاملة لحوكمة الشركات، أكثر من اهتمامها بالمسائل الخاصة بحوكمة تقنية المعلومات. ويتم تحديد هذه الأنشـطة من خلال الخطة السنوية للتدقيق الداخلي التي يتم إعدادها بواسطة وحدة التدقيق الداخلي والموافقة عليها واعتمادها من قبل لجنة التدقيق.

تعتبر المراجعات التي تقوم بهـا لجنة التدقيق لجميع خطط التدقيق الداخلي هامة وضرورية لتحديد السياسـات والخطط المسـتقبلية على نحو أكثر فاعلية. لذا يجب أن تتولى لجنة التدقيق هذا الدور التنسـيقي الرفيع المستوى، حتى تتمكن جميع الأطراف المعنية (كإدارة المؤسسـة، والمدققين الداخليين، والتدقيق الخارجي على حد سـواء) من تحقيق مستوى فهم ومعرفة أفضل لطبيعة وآلية مجمل خطة التدقيق الداخلي، وما يمكن توقعـه من مقدمي خدمات التدقيق. وعـلى الرغم من وجود قيود عملية على الكيفية أو الطريقة التي يمكن مـن خلالها إشراك لجنة التدقيق في العملية التفصيلية للتخطيط على نحو فعال، فإن بعض هذه المشـاركات أعطت قيمـة عالية لعملية التخطيط. وقد جرت العادة بأن يكون رئيس لجنة التدقيق هو الشـخص الأكثر فاعلية في هذه العملية الخاصة بمراجعة الخطة، ولكن حتى هذا الشـخص يتقيد في عمله هذا بمدد زمنية. لذا يجـب أن تقـوم وحدة التدقيق الداخلي بإعـداد وتحضير مجموعة كاملـة من الوثائق التفصيليـة المتعلقة بالخطط السـنوية، وأن تقوم بتقديمها للجنة التدقيق التي سـتقدم بدورها خططاً تفصيلية للسـنة القادمة وخططاً مسـتقبلية طويلة المدى. كما يجب أن تقوم وحدة التدقيق الداخلي أيضاً بإعداد تقارير موجزة عن أنشـطة التدقيق وعمليات إعادة التقييم السابقة للمناطق التي قامت بتدقيقها لإعطاء لجنة التدقيق صورة واضحة عن المناطق الهامة التي تمت تغطيها في المراجعات السـابقة. وعلى الرغم من أنه يجب على وحدة التدقيق الداخلي أن تقوم بإعداد تقرير خاص بأنشـطتها وإرسـاله إلى لجنة التدقيق بشـكل منتظم، فإن هذا التقرير الموجز للنشـاط السابق يعطي لمحة عامة عن المجـالات التي تركز عليها عملية التدقيق، ويسـلط الضوء أيضـاً على أي ثغرات يحتمل ظهورها وقت التدقيق.

ومن منظور حوكمة تقنية المعلومات، قد تتسبب خطط التدقيق الداخلي أحياناً في إثارة مشـاكل لأعضاء لجنة التدقيق في المؤسسـة. فغالباً ما يجهل هؤلاء الأشخاص أو المديرون

الرفيعو المستوى بعض المسائل المتعلقة بحوكمة تقنية المعلومات التي تم الحديث عنها في فصول هذا الكتــاب كإدارة معيار أمن البيانات الخاص بصناعة بطاقات الدفع PCI DSS، والــذي تحدثنا عنه في الفصل الحادي عشر من هذا الكتاب. لذا يجب على مدير التدقيق، وبدعم من الفريق الخاص بتدقيق تقنية المعلومات، أن يقوموا باتخاذ المزيد من الخطوات لتثقيف لجنة التدقيق عن ســبب تأكدها من أهمية القضايا الأكثر فنيةً التي تتعلق بتقنية المعلومات من منظور الضوابط الداخلية ومخاطر حوكمة تقنية المعلومات.

اجتماعات لجنة التدقيق وقضايا حوكمة تقنية المعلومات:

قد تكــون القضايا والمخاوف المتعلقــة بحوكمة تقنية المعلومات غير مألوفة بالنســبة لبعــض المديرين العاملين في لجــان التدقيق، وذلك من خلال بعــض القضايا التي تبدو في بعض الأحيان غريبة بالنسبة إليهم. ويعتاد المديرون التنفيذيون العاملون في لجنة التدقيق غالبــاً على التعامــل مع عدد محدود من القضايا المتعلقة بحوكمــة تقنية المعلومات حتى أصبحت مألوفة بالنســبة لهــم، مثل أهمية الخطط الفعالة لاســتمرارية تقنية المعلومات، والمســؤوليات القانونية المحتملة الناجمة عن قضايا حوسبة الشبكة الاجتماعية، أو المخاطر المتعلقــة بفيروســات البرمجيــات. وقد تحدثت العديد من منشــورات الأعــمال الموجهة للمديرين التنفيذيين في لجنــة التدقيق عن أنواع المخاطر وقضايا حوكمة تقنية المعلومات المتعلقة بها. ومع ذلك، فإنه يجب على كل من الإدارة العليا ومدير التدقيق ووحدة تدقيق تقنية المعلومات، أن يقوموا بمحاولة إيصال مخاوفهم المتعلقة بالقضايا الأكثر تقنية وقضايا الحوكمة المرتبطة بها إلى أعضاء لجنة التدقيق.

تعــد خطط مراجعة تدقيقــات حوكمة تقنية المعلومات والمخــاوف المتعلقة بالمخاطر جــزءاً من الخطــط الإجمالية لعمليات التدقيق الداخلي، لذا يجــب أن يكون هناك اتصال مفتوح بين مدققي تقنية المعلومات ومديريهم التنفيذيين فيما يخص تلك القضايا المحددة في حوكمــة تقنية المعلومات. ومع ذلك فإن إرســال الخطابــات إلى لجنة التدقيق تعتبر في بعض الأحيان مشــكلة كبيرة. وكما تحدثنا سابقاً، فإن أعضاء لجنة التدقيق مشغولون تماماً أكثر بالقضايا التي تتعلق بالتقارير المالية والالتزام بقانون ساربنز أوكسلي SOx وغيرها من قضايا المخاطر الأخرى، ولا يركز العديد منهم على قضايا التدقيق الداخلي المرتبطة بحوكمة

تقنية المعلومات بشــكل منتظم. وبالاســتعانة بمدير التدقيق، تحتاج عملية تدقيق تقنية المعلومــات إلى أن تصــل إلى أعضاء لجنــة التدقيق لتطلعهم على أهميــة القضايا المتعلقة بالضوابط الداخلية لحوكمة تقنية المعلومات ومدى تطورها.

وقــد يكون مــن المجدي أو من الأهمية بمكان بالنســبة للعديد من المؤسســات أن تقوم بجدولة اجتماعات توجيهية ربع ســنوية (كل ثلاثة أشــهر) مع لجنــة التدقيق لإطلاعهم على المخاطر والمســتجدات المتعلقة بحوكمة تقنية المعلومات. ويمكن اســتغلال هذه الاجتماعات لتثقيف أعضاء لجنة التدقيق عن قضايا بيئة حوكمة تقنية المعلومات في المؤسسة وغيرها من القضايا المتعلقة بالمخاطر. ويمكن أحياناً تنفيذ هذا النوع من الاجتماعات بالاشتراك مع المدير التنفيذي للمعلومات في المؤســـة، لكن في كثير من الأحيان نرى أنه من الأفضل أن يتم قيادة الجلسة في المقام الأول من قبل مدير التدقيق ووحدة تدقيق تقنية المعلومات في المؤسسة.

إن المســؤولية العظمى التي تقع على عاتق لجنة التدقيــق هي القيام بمراجعة النتائج الهامــة لعميات التدقيق التي تصل إليها عن طريق المدققين الداخليين والخارجيين والإدارة وغيرهم، وأن تقوم باتخاذ التدابير المناسبة حيالها. ومع أن لجنة التدقيق تتحمل المسؤولية عن كل هذه المجالات، إلا أن تركيزنا هنا ينصب على الحاجة إلى لجنة تدقيق تقوم بعمليات التدقيق الداخلي وتدقيق تقنية المعلومات على وجه الخصوص، وذلك لمراجعة وفهم جميع النتائج والقضايا المتعلقة بحوكمة تقنية المعلومات التي تصل لأعضاء اللجنة واتخاذ التدابير المناسبة المنتظمة والفورية.

إن الــرد على النتائج الهامة لعمليــة التدقيق التي تم إيصالها إلى لجنة التدقيق يتطلب مزيجــاً من الفهــم، والكفاءة، والتعاون من قبــل جميع الأطراف الرئيســية المعنية، وهي التدقيق الداخلي، والإدارة، والمدققين الخارجيين، ولجنة التدقيق نفســها. ويصبح بعد ذلك مستوى الرفاهية في المؤسسة هو المعيار الحقيقي الذي نحكم من خلاله على جميع خدمات التدقيق الداخلي، على عكس العديد من المرئيات المحلية التي ترى احتمالية تعارض مصالح كل من الإدارة ولجنة التدقيق. كما يجب على إدارة تقنية المعلومات، في حدود مسؤوليتها، أن تعمل بجد بتطبيق التدابير التحســينية المســتمرة للحوكمة لتقييــم ما إذا كانت البنود المناسبة للإجراء التصحيحي في مكانها الصحيح.

لقد تحدث هذا الفصل والفصول الســابقة من هذا الكتاب عن مجموعة واســعة من القضايا الخاصة بحوكمة تقنية المعلومات التي تؤثر في مؤسسات الأعمال. وعلى الرغم من أن لجنة التدقيق هي المسؤولة في نهاية المطاف عن تقييم التقدم والأنشطة المتعلقة بهذه الأمور، فإنه يجب على الإدارة العليا المســؤولة عن حوكمة تقنية المعلومات في المؤسسة أن تحدد ما إذا كان قد تم تثبيت ووضع العمليات المناسبة، وما إذا كانت تلك العمليات تعمل بالشكل الصحيح. إن النظام الجيد لضوابط وعمليات حوكمة تقنية المعلومات سوف يسهم في نجاح المؤسسة بشكل عام.

نبذة عن المؤلف:

روبرت ر. مولر، حاصل على شهادات CPA و CISA و CISSP وPMP، وهو متخصص في التدقيــق الداخــلي ونظم الرقابة الداخلية وإدارة المشــاريع، ولديــه فهم جيد لحوكمة الــشركات ونظم المعلومات وإدارة المخاطر. تمتد خبرته لأكثر من ٤٠ عاماً في إدارة وحدات التدقيق الداخلي وإدارة مجموعة واسعة من مشاريع تقنية المعلومات وغيرها من المشاريع مــن خلال نظم الرقابــة الداخلية والحوكمة. عمل مديراً وطنيــاً لتدقيق تقنية المعلومات لشركة جرانت ثورنتون (Grant Thornton)، كما كان مدير التدقيق الداخلي لشركة ســيرز روبــوك (Sears Roebuck)، حيث كان يرفع تقاريره للجنــة التدقيق وترأس فريقاً لإعادة هيكلة عمليات الرقابة الداخلية للمؤسسة وكان أول من أنشأ إدارة أخلاقيات شركتهم. يعد الكاتــب مؤلفاً ومتحدثاً مشــهوراً، فهو يقدم لقارئيــه رؤى ثاقبة لعديد من قضايا الأعمال ومخاوفها التي تؤثر في عمليات الحوكمة والمخاطر والامتثال في المؤسسة.

المترجم في سطور

١- محمد أحمد عبداللطيف أحمد

المؤهل العلمي:

• ماجستير علوم الحاسب، جامعة المنيا، مصر عام ٢٠٠٩ م.

العمل الحالي:

• عضو هيئة تدريب، قطاع تقنية المعلومات، معهد الإدارة العامة، الرياض.

الأنشطة العلمية والعملية:

- باحث بقسم علوم الحاسب، كلية العلوم، جامعة المنيا، ٢٠٠٤-٢٠٠٦.
- عضو فريق مشروع إنشاء مركز دعم نظم المعلومات الإدارية، جامعة المنيا، ٢٠٠٦ -٢٠١٠.
- تصميـم وإعداد ومراجعـة عدة حقائب تدريبيـة، معهد الإدارة العامـة – قطاع تقنية المعلومات.
- حاصل على العديد من الشـهادات الاحترافية الدولية في مجال تقنية المعلومات وإدارتها وحوكمتها.
- مدرب معتمد من شركة ميكروسوفت.

إضافة إلى هذا الكتاب لدى المترجم عدد من الأبحاث العلمية:

1- Ahmed. A. A. Radwan, Fatma A. Omara, A. A .Ali, M. A. Abdelatif, "Enhanced Distributed QoS Routing Algorithms in Wireless Networks", International Journal of Intelligent Computing & Information Sciences, Vol.8, No.2, (July2008) pp223-235

2- Ahmed. A. A. Radwan, Fatma A. Omara, A. A .Ali, M. A. Abdelatif, “Distributed QoS Routing Using Developed Flooding in Wireless Ad

Hoc Networks", The proceeding of the fourth International Conference on Intelligent Computing and Information Systems (ICICIS) 19-22 March 2009, pp. 490-501, Cairo-Egypt

3- Mohamed A. El-Sayed, M. Hassaballah, Mohammed A. Abdel-Latif, "Identity Verification of Individuals Based on Retinal Features Using Gabor Filters and SVM", Journal of Signal and Information Processing, Vol.7 No.1, February 2016, pp.49-59

4- Mohamed A. El-Sayed, Mohammed A. Abdel-Latif, "Optimization Methods for Identity Verification System Using Biometric Features", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 18 (2017) pp. 7143-7153

٢- عبدالله حسن كامل صالح

المؤهل العلمي:

- ماجستير في علوم الحاسب الآلي والبرمجة من الجامعة الأردنية، عمان، الأردن، عام ٢٠٠١ م.

العمل الحالي:

- مدرب في قطاع برامج الحاسب في معهد الإدارة العامة - المركز الرئيسي في الرياض.
- مسئول عن تقديم الدعم الفني والتقني للأنظمة المالية والموارد البشرية الخاصة بتطبيق أنظمة التخطيط للموارد المؤسسية ERP في معهد الإدارة العامة في المركز الرئيسي في الرياض.

الأنشطة العلمية والعملية:

- عضو هيئة تدريس (محاضر) في كلية تقنية المعلومات - جامعة فيلادلفيا في الأردن من عام ٢٠٠١ إلى عام ٢٠٠٨.
- عضو هيئة تدريب (مدرب) في معهد الإدارة العامة - المركز الرئيسي - الرياض من عام ٢٠٠٨ إلى الآن.
- تصميم ومراجعة عدة حقائب تدريبية في معهد الإدارة العامة -قطاع تقنية المعلومات.
- عضو في لجنة إعداد الخطة الإستراتيجية لتقنية المعلومات في معهد الإدارة العامة المنفذة منذ العام ١٤٣٦/١٤٣٥ هـ إلى عام ١٤٤٠ هـ.
- عضو في فريق إعداد معايير نشاط الاستشارات في معهد الإدارة العامة بالتنسيق مع الهيئة الوطنية للتقويم والاعتماد الأكاديمي في وزارة التعليم.

مراجع الترجمة في سطور

د. محمد بن عبدالله الشنيفي

المؤهل العلمي:

دكتوراه الفلسفة في علوم الحاسب الآلي، مايو ١٩٩٨،

معهد إلينوي للتكنولوجيا، شيكاغو، إلينوي.

العمل الحالي:

- أستاذ مشارك في قسم هندسة علوم الحاسب الآلي، كلية علوم الحاسب وتقنية المعلومات، جامعة الباحة. ديسمبر ٢٠١٦ إلى الوقت الحاضر.

أبرز لأنشطة العلمية:

- Hisham Al-Mubaid, Sasikanth Potu1, and M. Shenify. Determining Multifunctional Genes and Diseases in Human Using Gene Ontology. 9th International Conference on Bioinformatics and Computational Biology (BICOB 2017) Honolulu, Hawaii, USA. March 20 – 22, 2017.
- Duong B. Nguyen, Mohamed Shenify, and Hisham Al-Mubaid1. Biomedical Text Classification with Improved Feature Weighting Method. 8th International Conference on Bioinformatics and Computational Biology (BICoB) Las Vegas, Nevada, USA. April 4-6, 2016.
- H. Al-Mubaid. Mohamed Shenify and Sultan Aljahdali.Assessing Gene-Disease Relationship with Multifunctional Genes Using GO. Accepted paper. IEEE AICCSA 2016.
- H. Al-Mubaid,and Mohame Shenify . Improved Bayesian based method for classifying disease documents.WSCAR-2016
- Bassam Naji Al-Tamimi, Mohammed Shenify, Rahmat Budiarto, A New Algorithm For Protecting Mobile Home Network From IPv6 Routing Header Vulnerability In Mixed IP Networks, Journal of ICT, UUM Press, Vol. 14, 2015 (to appear)

- Mohamed Shenify and Foukrul Alom Mazarbhuiya. The Expected Value of Fuzzy Number. International Journal of Intelligence Science, 2015, Vol. 5, Pp. 1-5.
- M. Shenify. Extracting Cyclic Frequent Set from Fuzzy Temporal Data. 30th International Conference on Computers and Their Applications CATA-2015, March 9-11, 2015. Honolulu, Hawaii, USA.
- M. Shenify and F. A. Mazarbhuiya. Discovering Monthly Fuzzy Patterns. International Journal of Intelligence Science, 2015, Vol.5, Pp. 37-43.
- Ali Alshehri, Naif Hamed Almutairy, El-Sayed Osman, Mohamed Shenify and, Rahmat Budiarto, 2015, Improvement of Teaching Listening English as Secondary Language Using Student Response Systems, A Case Study at King Fahd Secondary School in Albaha: Towards Informed Teacher Decisions, Proceedings of the AlBaha University and Uppsala University Symposium on Quality in Computing Education (ABU3QCE 2015), Albaha, KSA, 24-25 February 2015, Pp.47-51 (http://www.abu3qce.al-aqiq.com/proceedings.pdf)
- Bassam Naji Al-Tamimi, Mohammed Shenify, Rahmat Budiarto, Protecting, Home Agent Client from IPv6 Routing Header Vulnerability in Mixed IP Networks , Journal of ICT, UUM Press, Vol. 14, 2015, Pp.77-93.
- Mohammed Shenify, Rahmat Budiarto, Sultan Aljahdali, Hisham M. Alsaghie,2015, Incorporating R&D Activities into Computer Engineering Teaching & Learning Program in Albaha University, Proceedings of The 3rd International Conference on Learning and Teaching in Computing and Engineering (LaTiCE, IEEE Technically Sponsored) 2015, Taipei, 9-12 April 2015
- F.A. Mazarbhuiya, M.Shenify. An Efficient Alogrithm for Minimg Locally Frequent Itemsets.2014 ASE BIGDAT/SOCIAL COM/CYBERSECURITY, Conference, Stanford University, May, 27-31, 2014. ISBN: 987-1-62561-000-3.
- Mohamed Shenify, Language Variation: Corpus Evaluation using Language Modeling, International Computing Conference in Arabic :ICCA 2013, 9-10-11, December, 2013.Tunisia.

- Mohamed Shenify Geographical Classification for Arabic text. International Computing Conference in Arabic :ICCA 2013, 9-10-11, December,2013 .Tunisia
- Mohamed Shenify, Trusted Node-Based Algorithm to Secure Home Agent NATed IPv4 Network from IPv6 Routing Header Attacks, TELKOMNIKA journal, Vol.12, No.4, December 2014, Pp. 969-976 (http://journal.uad.ac.id/index.php/TELKOMNIKA/article/view/540/pdf_51)
- Mohamed Shenify, Retrieving Information Using Concept For Multi-Format Data In Cloud Environment, Submitting to JTAIT
- Zahra Eskandari, Seyed Amin Hosseini Seno, Muhamed Shenify, Rahmat Budiarto, 2014, Optimal Cluster Head selection in Wireless Sensor Networks using Integer Linear Programming Techniques, International Journal of Informatics and Communication Technology (IJ-ICT), IAES ISSN: 2252-8776, Vol 3(3), DOI: 10.11591/ij-ict.v3i3.6614

  (http://iaesjournal.com/online/index.php/IJICT/article/view/6614
- Alireza Tajalli, Seyed-Amin Hosseini-Seno and, Mohamed Shenify, Rahmat Budiarto, 2014, An Incentive Mechanism for Cooperative Data Replication in MANETs A Game Theoretical Approach, Proceedings of International Conference Electrical Engineering, Computer Science and Informatics (EECSI 2014), Yogyakarta, Indonesia, 20-21 August 2014, Pp.111115 (http://iaesonline.com/eecsi/2014/)
- Fatemeh Hakimifar ,Seyed-Amin Hosseini-Seno, Mohamed Shenify and Rahmat Budiarto, 2014, An Efficient Cluster-based Routing Protocol for Mobile Ad Hoc Networks, Proceedings of International Conference Electrical Engineering, Computer Science and Informatics (EECSI 2014), Yogyakarta, Indonesia, 20-21 August 2014, Pp.476-481 (http://iaesonline.com/eecsi/2014/)
- F. A. Mazarbhuiya, M. Shenify, A. Khan, A. Farooq. Finding Cyclic Frequent Itemsets. IJCSI International Journal of Computer Science, 2012, Vol. 9, issue 6 (1), 229-236.
- Soraya Zaidi, Ahmed Abdelali, Mohamed-Tayeb Laskri, Mohamed A. Al Shenify. Extracting Simple and Compound Terms from Arabic Texts: An Application on The Quranic Text. Communication of the Arab Computer Society, 2011, vol. 4(1).

- Mu'away Naser and Mohammd Al-Shnify. Blood Vessels Segmentation From Lever CT Scan Image Using Level Set Curve Evolution. G. J. P&A Sc and Tech., 2011, vol. 1(2), Pp. 38-55.
- Mohammed Shenify, Rahmat Budiarto, Sultan Aljahdali, Hisham M. Alsaghie,2015, Incorporating R&D Activities into Computer Engineering Teaching & Learning Program in Albaha University, Proceedings of The 3rd International Conference on Learning and Teaching in Computing and Engineering (LaTiCE, IEEE Technically Sponsored) 2015, Taipei, 9-12 April 2015.

تم التصميم والإخراج الفني والطباعة في
الإدارة العامة للطباعة والنشر بمعهد الإدارة العامة - ١٤٤٠هـ

هذا الكتاب:

يزداد الاهتمـــام بالحوكمة من قِبل جميع الشـــركات على اختلاف أحجامها وأنواعها، سواء كانت مؤسسات قطاع عام لا تهدف للربح أم كيانات خاصة، وذلـــك في ظل الظروف الاقتصادية الدائمة التغير التي يشهدها عالم اليوم. وتتكون مفاهيم حوكمة المؤسسات من سلسلة من مجالات واســـعة تغطي جميع أنشطة المؤسســـة، والتي يتطلب تطبيقها عدداً من الإرشـــادات والبرامج لضمان نزاهة الإجراءات الإدارية وحماية المؤسسة من الممارسات المخالفة والاحتيالية. ومن الطبيعي أن تحتاج الحوكمة المؤسسية الفعالة إلى مهارات إدارية قوية لاتخاذ قرارات مهمة، كما تحتاج احتياجـــاً كبيراً إلى نظم وعمليات تقنية المعلومات علـــى وجه الخصوص. ويمثل هذا المجال المهـــم حوكمة تقنية المعلومات، وهو الموضوع الشامل لهذا الدليل التنفيذي.

يتناول هـــذا الكتاب مفهوم حوكمة تقنيـــة المعلومات، الذي يُعَد جزءاً من مفاهيم حوكمة المؤسسات، فهو يهدف إلى تقديم معلومات أساســـية عن القضايا المتعلقـــة بحوكمة تقنيـــة المعلومات. وقد تم تقســـيم الكتاب إلى ستة أجزاء رئيسية يتناول كلُّ جزء منها عدداً من القضايا التي تخص حوكمة تقنية المعلومات.

إن الهدف العام من هذا الكتاب يتمثل في مســـاعدة كبار مديري المؤســـسات على فهم أهمية قضايا حوكمـــة تقنية المعلومات فهماً أفضل وتطبيقها في مؤسســـاتهم، من خلال تزويدهم بالمعايير وأطر العمل العالمية اللازمة للوصول إلى نظم وعمليات أقوى لكلٍّ من تقنية المعلومات والمؤسسة بأكملها.

9960142876

تصميم وإخراج وطباعة الإدارة العامة للطباعة والنشر- معهد الإدارة العامة ١٤٤٠هـ